PRIVACY POLICY

Effective Date: November 1, 2025
Last Updated: November 1, 2025

---

1. INTRODUCTION

Welcome to Cartoform, a service operated by Traverse Labs LLC ("**Company**," "**we**," "**us**," or "**our**"). This Privacy Policy explains how we collect, use, disclose, and protect your personal information when you use our website, applications, and services (collectively, the "**Service**").

By accessing or using the Service, you agree to this Privacy Policy. If you do not agree with this Privacy Policy, please do not use the Service.

Contact Information:

- **Company Name:** Traverse Labs LLC
- **Address:** 487 N High Ridge Rd, Saratoga Springs, UT 84045
- **Email:** info@traverselabs.net
- **Support:** support@cartoform.com
- **Phone:** +1 712-318-3827

---

2. INFORMATION WE COLLECT

2.1 Information You Provide to Us

Account Information:

- Email address
- First and last name
- Password (stored in hashed form)
- Organization information
- Account preferences and settings

Project and Usage Data:

- Project names and descriptions
- Uploaded geospatial files (DEM, DSM, LIDAR, LAZ, LAS, GeoTIFF)
- URLs to external data sources you provide
- Region of Interest (ROI) coordinates
- STL generation parameters and settings
- Project processing status and history
- File sizes and storage usage metrics

Billing Information:

- Stripe customer ID
- Subscription tier and billing history
- Country code for pricing purposes
- Payment transaction records (credit card information is processed and stored by Stripe,

not by us)

Communications:

- Email addresses for notifications
- Email notification preferences
- Content of communications with our support team

2.2 Information We Collect Automatically

When you use the Service, we automatically collect certain information:

Technical Information:

- IP address (for geolocation, analytics, and abuse prevention)
- Browser type and version
- Device information and operating system
- Referring URLs and pages visited
- Clickstream data and time spent on pages
- Approximate geolocation data (derived from IP address)
- User activity data (mouse movements, clicks, scrolls) for session management and token refresh

Authentication Data:

- JWT tokens and refresh tokens
- Session data and authentication logs
- Password reset tokens (retained for 1 hour)
- Email verification codes (retained for 15 minutes)
- API client application IDs and secrets (for Premium tier users)

2.3 Cookies and Tracking Technologies

We use cookies, local storage, session storage, and similar tracking technologies:

Essential Cookies: Required for authentication and core Service functionality (e.g., storing authentication tokens).

Analytics Cookies: Used to understand how users interact with the Service through Plausible Analytics and Mixpanel (with PII redaction).

Third-Party Cookies: May be set by our third-party service providers.

You can control cookies through your browser settings. However, disabling essential cookies may limit your ability to use certain features of the Service. A cookie consent mechanism is planned for future implementation.

---

3. HOW WE USE YOUR INFORMATION

We use your information for the following purposes:

3.1 Service Delivery

- To create and manage your account

- To process and store your geospatial data and generate STL files
- To provide customer support and respond to your inquiries
- To authenticate users and maintain session security
- To enforce our Terms of Service and prevent fraud or abuse

3.2 Billing and Payments

- To process subscription payments through Stripe
- To manage billing accounts and subscription tiers
- To send purchase confirmations and billing notifications
- To maintain financial records as required by law

3.3 Communications

- To send transactional emails (account verification, password resets, project completion notifications)
- To send service-related announcements and updates
- To notify you of password expiration (90-day rotation policy)
- To respond to your requests and provide customer support

3.4 Service Improvement

- To analyze usage patterns and improve the Service
- To develop new features and functionality
- To train AI/ML models using company-owned content
- To conduct security monitoring and prevent abuse

3.5 Legal Compliance

- To comply with legal obligations and respond to lawful requests
- To protect our rights, property, and safety, and that of our users
- To enforce our Terms of Service and other agreements

---

4. HOW WE SHARE YOUR INFORMATION

4.1 Third-Party Service Providers

We share your information with trusted third-party service providers who assist us in operating the Service:

Stripe (Payment Processing)

- Purpose: Payment processing and subscription management
- Data Shared: Email, name, payment information, subscription details
- Privacy Policy: https://stripe.com/privacy
- Data Processing Agreement: Automatically applies per Stripe's terms

Amazon Web Services (AWS)

- Services: S3 (storage), SQS (queues), SES (email), RDS (database), EKS (compute), CloudWatch (monitoring), CloudTrail (logging)
- Region: Primarily us-east-2, expanding to other regions as needed

- Data Shared: All user-uploaded files, project data, email communications, application logs
- Privacy Policy: https://aws.amazon.com/privacy
- Data Processing Agreement: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Plausible Analytics

- Purpose: Web traffic and usage analytics
- Data Shared: IP addresses (anonymized), browser type, device information, pages visited, geolocation data
- PII Redaction: We do not send personally identifiable information to Plausible
- Privacy Policy: https://plausible.io/privacy
- Data Processing Agreement: https://plausible.io/dpa
- Opt-Out: Available through cookie consent settings

Mixpanel

- Purpose: Product usage analytics and event tracking
- Data Shared: IP addresses (anonymized), browser type, device information, usage patterns
- PII Redaction: We do not send personally identifiable information to Mixpanel
- Privacy Policy: https://mixpanel.com/legal/privacy-policy
- Data Processing Agreement: https://mixpanel.com/legal/dpa
- Opt-Out: Available through cookie consent settings

4.2 Data Sharing Practices

We DO NOT:

- Sell your personal information to third parties
- Share your data with affiliates or third parties for marketing purposes

We MAY share anonymized or aggregated data that does not identify you personally for analytics, research, and service improvement purposes.

4.3 Legal Disclosures

We may disclose your information:

- In response to lawful requests from law enforcement or government authorities
- To comply with applicable laws, regulations, or legal processes
- To protect our rights, property, safety, or that of our users or the public
- In connection with a business transfer, merger, acquisition, or sale of assets
- With your consent or at your direction

We have a law enforcement request policy that requires proper legal process before disclosing user information.

---

5. INTERNATIONAL DATA TRANSFERS

Cartoform is operated by Traverse Labs LLC, a U.S.-based company. Our services are intended primarily for users located in the United States. Our data is stored on AWS infrastructure primarily in the us-east-2 region.

If you access the Service from outside the United States, your information will be transferred to, stored, and processed in the United States and other countries where our service providers operate. These countries may have data protection laws that differ from those in your country.

For data transfers from the European Economic Area (EEA) or United Kingdom to the United States, we rely on Standard Contractual Clauses (SCCs) approved by the European Commission and UK authorities, as implemented through our agreements with AWS and other service providers.

By using the Service, you consent to the transfer of your information to the United States and other countries as described in this Privacy Policy.

---

6. DATA SECURITY

We implement reasonable technical, administrative, and physical security measures to protect your information from unauthorized access, disclosure, alteration, and destruction.

6.1 Security Measures

Authentication and Access Control:

- JWT token-based authentication with 1-hour session timeout
- Password hashing using industry-standard algorithms (BCrypt)
- Password complexity requirements (minimum 8 characters, uppercase, lowercase, digit, special character)
- Password rotation policy (90-day expiration)
- Password history tracking (prevents reuse of last 5 passwords)
- Role-based access control (RBAC)
- Organization-based access control
- Account lockout after failed login attempts
- API rate limiting to prevent abuse

Data Protection:

- Encryption at rest using AWS-managed encryption for S3, RDS, and SQS
- Encryption in transit using TLS/SSL enforced by load balancers
- Database encryption using AWS-managed encryption for RDS
- Secure file deletion procedures for user data

Monitoring and Incident Response:

- Security monitoring and logging via AWS CloudWatch and CloudTrail
- Intrusion detection through CloudTrail logging
- Incident response plan for security events
- Data breach notification procedures
- Occasional security audits and penetration testing

Application Security:

- CSRF (Cross-Site Request Forgery) protection
- XSS (Cross-Site Scripting) protection
- SQL injection prevention through JPA/Hibernate ORM
- Input validation and sanitization

6.2 Limitations

While we strive to protect your information, no security system is impenetrable. We cannot guarantee the absolute security of your information. You are responsible for maintaining the confidentiality of your account credentials and for any activity that occurs under your account.

---

7. DATA RETENTION

7.1 Retention Periods

We retain your information for as long as necessary to provide the Service and fulfill the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law.

Account Data:

- Active user accounts: Retained indefinitely until you request deletion
- Inactive user accounts: Retained indefinitely until you request deletion

Project Data:

- Hobby tier: 60 days from last activity
- Standard tier: 180 days from last activity
- Premium tier: Unlimited retention during active subscription

Financial Records:

- Billing and payment records: 7 years (legal requirement)

Communications and Logs:

- Email communications: 30 days
- Analytics and log data: 30 days
- Notification tracking records: 30 days

Security Tokens:

- Password reset tokens: 1 hour
- Email verification codes: 15 minutes
- Expired API client secrets: 90 days

Backups:

- Backup retention: 7 days

7.2 Automated Cleanup

We automatically delete:

- Expired password reset tokens (hourly cleanup)
- Stuck or failed batch jobs (15-minute check intervals)
- Old password history entries (beyond 5 most recent)
- Expired API client secrets (after 90-day retention period)

---

8. YOUR RIGHTS AND CHOICES

8.1 Access and Correction

You have the right to:

- **Access** your personal information through your account dashboard or API
- **Update** your email, name, password, and project information
- **Correct** inaccurate or incomplete information

Email verification is required when changing your email address.

8.2 Data Deletion

You have the right to:

- **Delete your account** by contacting customer support
- **Delete individual projects** through the Service interface
- **Delete uploaded files** through the Service interface

Upon account deletion, your data will be permanently deleted in accordance with our retention policies, except where we are required to retain certain information for legal, accounting, or security purposes (e.g., billing records retained for 7 years).

8.3 Data Portability

Currently, we do not offer automated data portability (data export) functionality. If you wish to obtain a copy of your data, please contact us at info@traverselabs.net, and we will respond within 30 days.

8.4 Communication Preferences

- **Transactional emails:** Required for account management and cannot be opted out
- **Notification emails:** Cannot be opted out (premium feature for customization)
- **Unsubscribe:** All emails include an unsubscribe link where applicable

8.5 Cookie Preferences

You can control cookies through your browser settings. Note that disabling essential cookies may limit Service functionality. A cookie consent mechanism is planned for future implementation.

8.6 Objection and Restriction (GDPR)

If you are located in the EEA or UK, you may have additional rights under the General Data Protection Regulation (GDPR), including the right to object to or restrict certain processing of your personal information. To exercise these rights, please contact us at info@traverselabs.net.

---

9. CHILDREN'S PRIVACY

The Service is not intended for children under the age of 13, and we do not knowingly collect personal information from children under 13. If we become aware that we have collected personal information from a child under 13, we will take steps to delete such information promptly.

If you believe we have collected information from a child under 13, please contact us at info@traverselabs.net.

---

10. CALIFORNIA PRIVACY RIGHTS (CCPA)

If you are a California resident, you may have additional rights under the California Consumer Privacy Act (CCPA), including:

- **Right to Know:** You have the right to request information about the categories and specific pieces of personal information we have collected about you, as well as the categories of sources, purposes for collection, and third parties with whom we share your information.
- **Right to Delete:** You have the right to request deletion of your personal information, subject to certain exceptions.
- **Right to Opt-Out:** You have the right to opt out of the "sale" of your personal information. We do not sell personal information as defined by the CCPA.
- **Right to Non-Discrimination:** You have the right not to receive discriminatory treatment for exercising your CCPA rights.

To exercise your CCPA rights, please contact us at info@traverselabs.net. We will verify your identity before processing your request and respond within 45 days.

Note: Our CCPA compliance is currently in progress. We are working to fully implement all CCPA requirements.

---

11. EUROPEAN PRIVACY RIGHTS (GDPR)

If you are located in the European Economic Area (EEA) or United Kingdom, you may have additional rights under the General Data Protection Regulation (GDPR), including:

- **Right of Access:** You have the right to obtain confirmation of whether we process your personal data and to access such data.
- **Right to Rectification:** You have the right to correct inaccurate or incomplete personal data.
- **Right to Erasure:** You have the right to request deletion of your personal data under certain circumstances.
- **Right to Restriction:** You have the right to restrict processing of your personal data under certain circumstances.

- **Right to Data Portability:** You have the right to receive your personal data in a structured, commonly used, and machine-readable format.
- **Right to Object:** You have the right to object to processing of your personal data under certain circumstances.
- **Right to Withdraw Consent:** Where processing is based on consent, you have the right to withdraw consent at any time.
- **Right to Lodge a Complaint:** You have the right to lodge a complaint with a supervisory authority.

To exercise your GDPR rights, please contact us at info@traverselabs.net. We will respond to your request within one month.

Legal Basis for Processing:

- **Contract Performance:** Processing necessary to provide the Service under our Terms of Service
- **Legitimate Interests:** Processing necessary for our legitimate business interests (e.g., fraud prevention, service improvement)
- **Legal Obligation:** Processing necessary to comply with legal requirements
- **Consent:** Where you have provided consent for specific processing activities

Note: Our GDPR compliance is currently in progress. We are working to fully implement all GDPR requirements.

---

12. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. When we make material changes, we will:

- Update the "Last Updated" date at the top of this Privacy Policy
- Notify you via email (optional) and/or a prominent notice on our website
- Provide at least 30 days' advance notice before the changes take effect
- Require re-acceptance for material changes

Your continued use of the Service after the effective date of the revised Privacy Policy constitutes your acceptance of the changes. If you do not agree to the revised Privacy Policy, you must stop using the Service.

We will maintain previous versions of this Privacy Policy for your reference.

---

13. CONTACT US

If you have any questions, concerns, or requests regarding this Privacy Policy or our privacy practices, please contact us:

Traverse Labs LLC
487 N High Ridge Rd
Saratoga Springs, UT 84045
United States

Email: info@traverselabs.net
Support: support@cartoform.com
Phone: +1 712-318-3827

For data protection inquiries, please email: info@traverselabs.net

---

14. ADDITIONAL INFORMATION

14.1 Do Not Track Signals

Some browsers include a "Do Not Track" (DNT) feature that signals to websites that you do not want your online activities tracked. We do not currently respond to DNT signals.

14.2 Third-Party Links

The Service may contain links to third-party websites or services. We are not responsible for the privacy practices of these third parties. We encourage you to review their privacy policies before providing any information to them.

14.3 Data Breach Notification

In the event of a data breach that affects your personal information, we will notify you and relevant authorities as required by applicable law. Our incident response plan includes procedures for assessing, containing, and remediating security incidents.

END OF PRIVACY POLICY

This Privacy Policy is effective as of November 1, 2025.