

Privacy Policy

Echoframe Media LLC — KeyBeam Studio

Last Updated: 2026-07-14

Effective Date: 2026-07-14

Echoframe Media LLC ("Echoframe," "we," "us," or "our") operates the KeyBeam Studio laser control software platform and related services. This Privacy Policy explains how we collect, use, store, share, and protect your personal information when you use KeyBeam Studio, visit our website, create an account, or otherwise interact with our services.

By using KeyBeam Studio, creating an account, activating a License Key, or visiting our website, you acknowledge that you have read and understand this Privacy Policy.

1. Who We Are

Echoframe Media LLC is a Colorado limited liability company with its principal place of business at:

8335 Fairmount Drive, Unit 1-104 Denver, Colorado, USA

Email: privacy@keybeam.studio

EU Representative (Article 27 GDPR): Where Article 27 GDPR applies, Echoframe will appoint and publish details of its EU Representative in this section.

UK Representative (Article 27 UK GDPR): Where Article 27 UK GDPR applies, Echoframe will appoint and publish details of its UK Representative in this section.

For questions about this Privacy Policy or your personal data, contact us at the email address above. If you are located in the European Economic Area ("EEA") or the United Kingdom ("UK"), you may also contact our representative in your jurisdiction.

2. Information We Collect

We collect information in the following categories:

2.1 Account Information. When you create a KeyBeam Studio account, we collect:

- (i) name;
- (ii) email address;
- (iii) username or display name; and
- (iv) password (stored in hashed form only).

2.2 Payment Information. When you purchase a subscription or lifetime license, payment is processed through Stripe, Inc. We do not directly collect or store your full credit card number, debit

card number, or bank account details. Stripe collects and processes your payment information under its own privacy policy. We receive from Stripe:

- (i) transaction confirmation and amount;
- (ii) last four digits of your payment method;
- (iii) billing country; and
- (iv) transaction ID and status.

2.3 License and Activation Data. When you activate the Software, we collect:

- (i) License Key and license type (trial, subscription, or lifetime);
- (ii) activation date and status;
- (iii) license expiration or renewal dates;
- (iv) device identifier or hardware fingerprint used for activation; and
- (v) activation server connection timestamps.

2.4 Software and Device Information. When you use the Software, we may automatically collect:

- (i) Software version number;
- (ii) operating system type and version;
- (iii) device type and hardware specifications relevant to Software performance;
- (iv) language and locale settings; and
- (v) IP address (used for license validation and geographic compliance).

2.5 Usage Analytics. We may collect general usage data to improve the Software, including:

- (i) features accessed and frequency of use;
- (ii) session duration and frequency;
- (iii) user interface interactions; and
- (iv) general workflow patterns.

We do not collect the content of DMX signals transmitted by the Software to connected hardware. We do not monitor, record, or analyze your lighting designs, show files, fixture configurations, or creative output.

2.6 Error and Crash Reports. If the Software encounters an error or crash, we may automatically collect:

- (i) error type and diagnostic code;

- (ii) Software state at the time of the error;
- (iii) operating system and hardware information; and
- (iv) stack traces or log excerpts that do not contain personal content.

2.7 Support Communications. When you contact us for support, we collect the content of your communications, including email address, name, and any information you provide in your support request.

2.8 Website Data. When you visit our website, we may collect standard web analytics data through cookies and similar technologies, including IP address, browser type, referring URL, pages visited, and time spent on the site.

3. How We Use Your Information

We use the information we collect for the following purposes:

3.1 License Management. To validate your License Key, manage your subscription, process activations, enforce license terms, and prevent unauthorized use.

3.2 Payment Processing. To process transactions, issue receipts, manage refunds, and maintain billing records.

3.3 Software Delivery and Updates. To deliver the Software, provide updates, patches, and new versions, and notify you of changes to the Software or your license.

3.4 Support. To respond to your support requests, troubleshoot issues, and provide technical assistance.

3.5 Software Improvement. To analyze usage patterns, identify bugs, improve performance, develop new features, and enhance the user experience.

3.6 Security and Fraud Prevention. To detect, investigate, and prevent unauthorized access, piracy, license abuse, fraud, and other threats to the integrity of our Software and systems.

3.7 Legal Compliance. To comply with applicable laws, regulations, legal processes, or government requests.

3.8 Communications. To send you service-related communications, including license expiration notices, update notifications, security alerts, and changes to our terms or policies. We do not send unsolicited marketing emails unless you have opted in.

3.9 Agreement Enforcement. To enforce our End-User License Agreement, including remote deactivation of License Keys in accordance with the EULA.

4. Lawful Bases for Processing (EEA and UK Users)

If you are located in the EEA or the UK, we are required to identify a lawful basis for each processing activity under the General Data Protection Regulation ("GDPR") and the UK General Data Protection Regulation ("UK GDPR"). The following table sets out the lawful basis we rely on for each category of processing:

4.1 Contract Performance (Article 6(1)(b) GDPR). We process the following data as necessary to perform our contract with you (the End-User License Agreement):

- (i) account information — to create and maintain your account;
- (ii) payment information — to process your purchase and manage billing;
- (iii) license and activation data — to validate your license, activate the Software, and manage your subscription or lifetime license;
- (iv) software and device information — to deliver the Software, provide updates, and ensure compatibility; and
- (v) support communications — to respond to your support requests and fulfill our support obligations.

4.2 Legitimate Interests (Article 6(1)(f) GDPR). We process the following data on the basis of our legitimate interests, which we have balanced against your rights and freedoms:

- (i) usage analytics — to improve the Software, develop features, and enhance the user experience (legitimate interest: product improvement);
- (ii) error and crash reports — to identify and fix bugs, improve stability, and maintain Software quality (legitimate interest: product quality and reliability);
- (iii) security monitoring and license enforcement — to detect piracy, prevent fraud, enforce license terms, and protect our intellectual property (legitimate interest: security and IP protection);
- (iv) IP address and geographic data — to comply with export controls and territorial licensing restrictions (legitimate interest: legal compliance and license integrity); and
- (v) website analytics — to understand how visitors interact with our website and improve its content and functionality (legitimate interest: website improvement).

You have the right to object to processing based on legitimate interests at any time. See Section 8 for how to exercise this right.

4.3 Legal Obligation (Article 6(1)(c) GDPR). We process data as necessary to comply with legal obligations, including tax and accounting record-keeping, export compliance, and responses to lawful government requests.

4.4 Consent (Article 6(1)(a) GDPR). We rely on consent for:

- (i) non-essential cookies and website tracking technologies (consent collected via our cookie consent mechanism); and

(ii) marketing communications, if and when offered (opt-in only).

You may withdraw consent at any time without affecting the lawfulness of processing carried out before withdrawal. To withdraw consent, adjust your cookie preferences on our website or contact us at the email address in Section 1.

5. Information Sharing

We do not sell your personal information. We share your information only in the following circumstances:

5.1 Payment Processor. We share transaction-related information with Stripe, Inc. to process payments. Stripe's handling of your data is governed by Stripe's privacy policy, available at stripe.com/privacy. Stripe acts as an independent data controller for payment data it collects directly from you, and as a data processor for transaction data we share with it.

5.2 Authorized Distributors. If you purchased a KeyBeam Studio license as part of a hardware bundle from an authorized distributor, the distributor may have your hardware purchase and delivery information from its own sales records. We do not share your software activation account, licensing history, subscription details, support records, or usage data with distributors unless required by law or authorized by you. Our distributors' collection of hardware customer information is governed by their own privacy policies.

5.3 Service Providers (Data Processors). We may share information with third-party service providers who perform services on our behalf, such as hosting, analytics, email delivery, and customer support tools. These providers process your data only on our instructions and are bound by data processing agreements that require them to implement appropriate security measures and use your information only to provide services to us. A current list of sub-processors is available upon request by contacting us at the email address in Section 1.

5.4 Legal Requirements. We may disclose your information if required by law, regulation, legal process, subpoena, court order, or government request, or if we believe disclosure is necessary to protect our rights, your safety, or the safety of others.

5.5 Business Transfers. In the event of a merger, acquisition, reorganization, sale of assets, or bankruptcy, your information may be transferred as part of the transaction. We will notify you of any such transfer and any changes to this Privacy Policy.

5.6 With Your Consent. We may share your information with third parties when you have given us explicit consent to do so.

6. International Data Transfers

6.1 Processing Location. KeyBeam Studio is operated from the United States. If you are located outside the United States, including in the EEA, the UK, or Switzerland, your personal data will be transferred to, stored in, and processed in the United States.

6.2 EU-US Data Privacy Framework. Where applicable, Echoframe may rely on certification under the EU-US Data Privacy Framework ("DPF"), the UK Extension to the DPF, and the Swiss-US Data Privacy Framework. If and when certified, we will publish certification details and status in this section.

6.3 Standard Contractual Clauses. Where the DPF does not apply or as a supplementary safeguard, we use Standard Contractual Clauses ("SCCs") adopted by the European Commission (and the UK International Data Transfer Agreement or Addendum, as applicable) as the legal mechanism for transferring personal data from the EEA and the UK to the United States. Copies of the applicable SCCs are available upon request.

6.4 Adequacy and Safeguards. We will not transfer personal data from the EEA or the UK to any country that has not received an adequacy decision from the European Commission or the UK Secretary of State, as applicable, unless appropriate safeguards are in place as required by applicable law.

7. Data Retention

7.1 Account Data. We retain your account information for as long as your account is active and for a reasonable period thereafter to fulfill legal, accounting, and business obligations.

7.2 License Records. We retain license activation records, licensing history, and transaction records for a minimum of three (3) years following the expiration or termination of your license, or longer as required by applicable law.

7.3 Usage Analytics. Usage analytics data is retained in aggregated or de-identified form and is not subject to individual deletion requests once aggregated.

7.4 Support Records. Support communications are retained for a reasonable period to maintain service quality and resolve recurring issues.

7.5 Retention Criteria. In determining retention periods, we consider the purpose for which data was collected, the sensitivity of the data, the risk of harm from unauthorized use or disclosure, applicable legal requirements, and whether the purpose can be fulfilled through anonymized data.

7.6 Deletion. When your data is no longer needed for the purposes described in this Privacy Policy, we will delete or de-identify it within a commercially reasonable timeframe, subject to legal and contractual retention obligations.

8. Your Privacy Rights

Depending on where you live, you may have certain rights regarding your personal information. We honor the following rights for all users, regardless of location, to the extent applicable:

8.1 Access. You may request a copy of the personal information we hold about you.

8.2 Correction. You may request that we correct inaccurate or incomplete personal information.

8.3 Deletion. You may request that we delete your personal information, subject to exceptions for data we are required or permitted to retain by law or for legitimate business purposes (such as license records and transaction history).

8.4 Data Portability. Where technically feasible, you may request a copy of your personal information in a structured, commonly used, and machine-readable format.

8.5 Opt-Out of Sale. We do not sell your personal information. If our practices change in the future, we will provide an opt-out mechanism as required by applicable law.

8.6 Non-Discrimination. We will not discriminate against you for exercising your privacy rights.

To exercise any of these rights, contact us at the email address listed in Section 1. We will respond to verified requests within the timeframe required by applicable law, generally within forty-five (45) days.

9. Additional Rights for EEA and UK Users

If you are located in the EEA or the UK, you have the following additional rights under the GDPR and UK GDPR:

9.1 Right to Restriction of Processing. You may request that we restrict the processing of your personal data in certain circumstances, including where you contest the accuracy of the data, where processing is unlawful but you oppose deletion, where we no longer need the data but you require it for the establishment, exercise, or defense of legal claims, or where you have objected to processing pending verification of our legitimate grounds.

9.2 Right to Object. You have the right to object to the processing of your personal data based on our legitimate interests (Section 4.2) at any time. Upon receiving your objection, we will cease processing your data for the relevant purpose unless we demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or the processing is necessary for the establishment, exercise, or defense of legal claims.

9.3 Right to Object to Direct Marketing. You have the absolute right to object to the processing of your personal data for direct marketing purposes at any time. If you exercise this right, we will stop processing your data for direct marketing immediately.

9.4 Right to Withdraw Consent. Where processing is based on consent (Section 4.4), you may withdraw your consent at any time. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

9.5 Automated Decision-Making. You have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning you or similarly significantly affects you. We do not currently engage in solely automated decision-making that produces legal or similarly significant effects.

9.6 Right to Lodge a Complaint. If you believe that our processing of your personal data violates the GDPR or UK GDPR, you have the right to lodge a complaint with a supervisory authority. You may file a complaint with the supervisory authority in the EU member state of your habitual residence, place of work, or place of the alleged infringement. For UK residents, the relevant authority is the Information Commissioner's Office (ICO) at ico.org.uk.

9.7 Response Time. We will respond to all rights requests from EEA and UK users within one (1) month of receipt. If a request is complex or we receive a high volume of requests, we may extend this period by up to two (2) additional months, and we will notify you of such extension and the reasons for it within the initial one-month period.

9.8 Identity Verification. We may request information necessary to verify your identity before fulfilling a rights request. We will not request more information than is necessary for verification purposes.

9.9 No Fee. We will fulfill your rights requests free of charge. We reserve the right to charge a reasonable fee or refuse to act on requests that are manifestly unfounded or excessive, particularly if repetitive.

10. Colorado Privacy Act

If you are a Colorado resident, the Colorado Privacy Act (CPA) provides you with specific rights regarding your personal data, including the right to access, correct, delete, and obtain a portable copy of your data, as well as the right to opt out of targeted advertising, the sale of personal data, and profiling in furtherance of decisions that produce legal or similarly significant effects.

We do not sell personal data. We do not engage in profiling that produces legal or similarly significant effects. If you wish to exercise your CPA rights, contact us at the email address in Section 1. If we decline your request, you may appeal by contacting us at the same address, and we will respond to your appeal within forty-five (45) days.

11. California Privacy Rights

If you are a California resident, the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), provides you with additional rights regarding your personal information.

11.1 Right to Know. You have the right to request that we disclose the categories and specific pieces of personal information we have collected about you, the categories of sources, the business purpose for collection, and the categories of third parties with whom we share your information.

11.2 Right to Delete. You have the right to request deletion of your personal information, subject to certain exceptions.

11.3 Right to Correct. You have the right to request correction of inaccurate personal information.

11.4 Right to Opt Out of Sale or Sharing. We do not sell or share your personal information for cross-context behavioral advertising.

11.5 No Discrimination. We will not discriminate against you for exercising your CCPA/CPRA rights.

11.6 Authorized Agents. You may designate an authorized agent to make requests on your behalf. We may require verification of the agent's authority.

11.7 Categories of Information. In the preceding twelve (12) months, we have collected the following categories of personal information: identifiers (name, email, IP address, device identifiers), commercial information (transaction history, license records), internet or electronic network activity (usage analytics, error reports, website browsing data), and geolocation data (IP-based location).

To exercise your California privacy rights, contact us at the email address in Section 1.

12. Data Security

We implement commercially reasonable administrative, technical, and physical security measures to protect your personal information against unauthorized access, alteration, disclosure, or destruction. These measures include:

- (i) encryption of data in transit using TLS/SSL;
- (ii) encryption of sensitive data at rest;
- (iii) secure hashing of passwords;
- (iv) access controls limiting personnel access to personal data on a need-to-know basis;
- (v) regular security assessments and vulnerability monitoring; and
- (vi) incident response procedures for identifying and addressing data breaches.

No method of electronic transmission or storage is completely secure. While we strive to protect your information, we cannot guarantee absolute security.

13. Data Breach Notification

13.1 EEA and UK Users. In the event of a personal data breach affecting data of EEA or UK users, we will notify the relevant supervisory authority without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to your rights and freedoms. Where a breach is likely to result in a high risk to your rights and freedoms, we will also notify you directly without undue delay.

13.2 US Users. We will comply with applicable state data breach notification laws, including the Colorado Consumer Protection Act breach notification requirements and the California Civil Code Section 1798.82 notification requirements, as applicable.

13.3 General. We maintain a documented data breach response plan that includes procedures for identifying, containing, assessing, and reporting data breaches.

14. Children's Privacy

KeyBeam Studio is not directed to children under the age of sixteen (16). We do not knowingly collect personal information from children under sixteen. If we become aware that we have collected personal information from a child under sixteen, we will take steps to delete that information promptly. If you believe a child under sixteen has provided us with personal information, please contact us at the email address in Section 1.

15. Cookies and Tracking Technologies

15.1 Website Cookies. Our website may use cookies and similar tracking technologies to enhance your browsing experience, analyze site traffic, and understand usage patterns. Cookies are small text files stored on your device.

15.2 Types of Cookies. We may use:

- (i) essential cookies necessary for website functionality;
- (ii) analytics cookies to understand how visitors interact with our website; and
- (iii) preference cookies to remember your settings and choices.

15.3 EEA and UK Users — Cookie Consent. If you are located in the EEA or the UK, we will not place non-essential cookies on your device without your prior opt-in consent. Our cookie consent mechanism allows you to accept or reject each category of non-essential cookies before they are set. You may change your preferences at any time through our cookie settings panel on our website. Essential cookies that are strictly necessary for the operation of the website do not require consent.

15.4 Software Telemetry. The Software may transmit usage analytics and error reports as described in Sections 2.5 and 2.6. This telemetry does not use browser cookies.

15.5 Your Choices. You can control cookies through your browser settings. Disabling certain cookies may affect website functionality. Software telemetry settings, if configurable, are managed within the Software's preferences.

16. Third-Party Links and Services

The Software or our website may contain links to third-party websites, services, or products. This Privacy Policy does not apply to third-party services. We are not responsible for the privacy practices of third parties. We encourage you to review the privacy policies of any third-party services you access.

17. What We Do Not Collect

For clarity, we want to be explicit about information we do not collect:

- (i) We do not collect the content of DMX signals you transmit through the Software.
- (ii) We do not monitor, record, or analyze your lighting designs, show files, cue lists, or creative output.
- (iii) We do not collect or store full credit card numbers, debit card numbers, or bank account details (payment processing is handled entirely by Stripe).
- (iv) We do not collect biometric data.
- (v) We do not collect information about your race, ethnicity, religion, sexual orientation, or political opinions.
- (vi) We do not process special categories of personal data as defined in Article 9 of the GDPR.

18. Data Protection Officer

Based on the nature and scale of our current data processing activities, we have determined that the appointment of a Data Protection Officer is not required under Article 37 of the GDPR. We will reassess this determination as our business grows and our processing activities evolve. In the interim, all data protection inquiries may be directed to:

Echoframe Media LLC 8335 Fairmount Drive, Unit 1-104 Denver, Colorado, USA Email:
[] Email: privacy@keybeam.studio

19. 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 business operations. When we make material changes, we will:

- (i) update the "Last Updated" date at the top of this policy;
- (ii) notify you through the Software or by email to the address associated with your account; and
- (iii) where required by applicable law, including the GDPR, obtain your consent before applying material changes to information previously collected under a prior version of this policy.

Your continued use of the Software after the effective date of a revised Privacy Policy constitutes your acceptance of the updated terms, except where applicable law requires express consent.

20. Contact Us

If you have questions about this Privacy Policy, your personal data, or wish to exercise any of your privacy rights, contact us at:

Echoframe Media LLC 8335 Fairmount Drive, Unit 1-104 Denver, Colorado, USA Email:
[] Email: privacy@keybeam.studio

EEA Users: You may also contact our EU Representative at: Where Article 27 GDPR applies, representative details will be published in Section 1.

UK Users: You may also contact our UK Representative at: Where Article 27 UK GDPR applies, representative details will be published in Section 1.

We will respond to all privacy-related inquiries within a commercially reasonable timeframe and within the periods required by applicable law (one month for GDPR/UK GDPR requests, forty-five days for US state law requests).