

Privacy Policy

Last Updated: January 18, 2026

1. INTRODUCTION

1.1 Overview

Welcome to DegenCreators. This Privacy Policy explains how DegenCreators, LLC (“DegenCreators,” “we,” “us,” or “our”) collects, uses, discloses, and protects your personal information when you access or use our Platform, including our website, mobile applications, and related services (collectively, the “Platform” or “Services”).

DegenCreators is committed to protecting your privacy and ensuring transparency about our data practices. This Privacy Policy is designed to help you understand:

- What information we collect and why we collect it
- How we use and share that information
- The choices you have regarding your information
- How we protect your information
- Your rights under applicable privacy laws

By accessing or using the Platform, you acknowledge that you have read and understood this Privacy Policy and consent to our collection, use, and disclosure of your personal information as described herein.

1.2 Scope

This Privacy Policy applies to all users of the Platform, including:

- Visitors who browse the Platform without creating an account
- Registered users with Subscriber accounts
- Creators who upload and monetize content
- Platform Token holders
- NFT buyers and sellers
- Anyone who interacts with our Services

This Privacy Policy is incorporated into and subject to our Terms of Service. Capitalized terms not defined in this Privacy Policy have the meanings given in our Terms of Service.

1.3 Updates 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
- Post the revised Privacy Policy on the Platform
- Notify you via email to the address associated with your account

- Display a prominent notice on the Platform
- Provide at least thirty (30) days' notice before material changes take effect (where required by law)

Your continued use of the Platform after the effective date of any changes constitutes your acceptance of the revised Privacy Policy. We encourage you to review this Privacy Policy periodically to stay informed about how we protect your information.

1.4 Contact Information

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

****Privacy Officer****
DegenCreators, LLC
[Address]
Email: privacy@degencreators.com
Phone: [Phone Number]

For users in the European Economic Area (EEA), United Kingdom (UK), or Switzerland, our data protection officer can be reached at: dpo@degencreators.com

2. INFORMATION WE COLLECT

2.1 Information You Provide Directly

We collect information that you voluntarily provide to us when you:

2.1.1 Create an Account

When you register for an account, we collect:

- ****Account Credentials:**** Username, email address, password (encrypted)
- ****Profile Information:**** Display name, profile picture, banner image, bio/description, social media links, website URL, pronouns, location (optional)
- ****Account Type:**** Creator or Subscriber designation
- ****Date of Birth:**** To verify you meet age requirements
- ****Country/Region:**** For compliance and content restriction purposes
- ****Referral Information:**** Referral codes or affiliate links (if applicable)

2.1.2 Identity Verification (Creators)

For Creator account verification, we collect:

- ****Government-Issued ID:**** Passport, driver's license, national ID card, or other official identification documents
- ****Verification Photos:**** Selfie with ID, biometric data from facial recognition
- ****Legal Name:**** As it appears on official documents
- ****Proof of Address:**** Utility bills, bank statements, or government correspondence
- ****Tax Information:**** Social Security Number (SSN), Taxpayer Identification Number (TIN), Individual Taxpayer Identification Number (ITIN), W-9 form, W-8BEN form, or equivalent tax documentation

- **Business Information:** Business name, entity type, business registration documents (if applicable)
- **Additional Documentation:** As may be required for enhanced verification or regulatory compliance

We use trusted third-party identity verification services to process this information. By submitting verification documents, you authorize us to share your information with these services.

2.1.3 Payment and Financial Information

When you make purchases or set up payouts, we collect:

- **Cryptocurrency Wallet Addresses:** Public wallet addresses you connect to the Platform
- **Payment Method Information:** Credit/debit card details (processed by third-party payment processors; we do not store full card numbers)
- **Bank Account Information:** Account and routing numbers for fiat payouts
- **Payment History:** Records of transactions, purchases, subscriptions, tips, and payouts
- **Billing Address:** For payment processing and tax purposes
- **Transaction Data:** Amounts, dates, recipients, and purposes of transactions

Note: We do not store your full credit card numbers or bank account credentials. Payment processing is handled by PCI-DSS compliant third-party processors. For cryptocurrency transactions, we only collect public wallet addresses; we never have access to your private keys.

2.1.4 Content You Upload

When you upload content as a Creator, we collect:

- **Creator Content:** Images, videos, audio files, text, and other media you upload
- **Content Metadata:** Titles, descriptions, tags, categories, pricing information, access restrictions
- **Model Release Forms:** Documentation of consent from individuals appearing in your content
- **Age Verification Records:** Proof of age for all performers (maintained by Creator, accessible for compliance verification)
- **NFT Information:** NFT metadata, smart contract parameters, royalty settings, collection details

2.1.5 Communications

When you communicate with us or other users, we collect:

- **Direct Messages:** Content of messages exchanged with other users through the Platform
- **Support Requests:** Information you provide when contacting customer support
- **Feedback and Surveys:** Responses to surveys, polls, or feedback requests
- **Emails:** Correspondence sent to our email addresses
- **Comments and Interactions:** Public comments, likes, ratings, or other interactions with content

2.1.6 Other Information You Provide

- **Preferences and Settings:** Notification preferences, privacy settings, content preferences, display settings
- **Subscription Information:** Subscription tiers, active subscriptions, subscription history
- **Dispute Information:** Information provided in connection with disputes, chargebacks, or appeals
- **Marketing Preferences:** Opt-in/opt-out choices for marketing communications
- **Contest or Promotion Entries:** Information submitted when participating in contests or promotions

2.2 Information Collected Automatically

When you access or use the Platform, we automatically collect certain information:

2.2.1 Device and Technical Information

- **Device Information:** Device type, model, operating system, browser type and version, device identifiers (UDID, IDFA, Android ID)
- **IP Address:** Your Internet Protocol address and general geographic location derived from it
- **Network Information:** Internet service provider, connection type, network status
- **Mobile Network Information:** Mobile carrier, phone number (in some cases)
- **Hardware Information:** Screen resolution, processor type, available storage

2.2.2 Usage Information

- **Access Logs:** Pages viewed, features used, time and date of access, time spent on pages
- **Click Data:** Links clicked, buttons pressed, navigation paths
- **Content Interactions:** Content viewed, downloaded, liked, shared, or commented on
- **Search Queries:** Terms you search for on the Platform
- **Session Information:** Login/logout times, session duration, frequency of visits
- **Performance Data:** Loading times, errors encountered, crashes, system performance

2.2.3 Location Information

- **Precise Location:** GPS coordinates (only if you grant permission through device settings)
- **Approximate Location:** Derived from IP address, Wi-Fi access points, or cell tower triangulation
- **Location Preferences:** Locations you specify in your profile or settings

We use location information to:

- Provide location-based features and content
- Comply with geographic content restrictions
- Detect fraud and unusual activity
- Improve our services
- Comply with legal obligations

You can control location permissions through your device settings, though this may limit certain features.

2.2.4 Cookies and Tracking Technologies

We use cookies, web beacons, pixels, local storage, and similar tracking technologies to collect information about your interactions with the Platform. See Section 2.4 for detailed information about cookies.

2.3 Blockchain and Cryptocurrency Information

When you engage in cryptocurrency or NFT transactions, we collect:

- ****Wallet Addresses:**** Public addresses of wallets you connect to the Platform
- ****Transaction Hashes:**** Unique identifiers of blockchain transactions
- ****Smart Contract Interactions:**** Records of your interactions with smart contracts
- ****Gas Fees:**** Information about transaction fees paid
- ****Token Holdings:**** Records of Platform Tokens or NFTs you own (publicly available on blockchain)
- ****Transaction Amounts:**** Values of cryptocurrency transactions
- ****Blockchain Network:**** Which blockchain networks you use (Ethereum, Polygon, etc.)
- ****NFT Metadata:**** Information about NFTs you create, buy, or sell

****Important:**** Blockchain transactions are public and permanent. Information recorded on the blockchain, including wallet addresses and transaction details, cannot be deleted or modified. While we collect and display this information, it is inherently public and accessible to anyone with blockchain analysis tools.

2.4 Cookies and Similar Technologies

2.4.1 Types of Cookies We Use

****Essential Cookies (Always Active):****

- Session management and authentication
- Security and fraud prevention
- Platform functionality and features
- Load balancing and performance optimization

These cookies are necessary for the Platform to function and cannot be disabled without impairing core functionality.

****Analytics Cookies (Optional):****

- Usage statistics and traffic analysis
- Feature performance measurement
- User behavior patterns
- A/B testing and optimization

****Functional Cookies (Optional):****

- Preference storage (language, theme, layout)
- Content recommendations
- Customized user experience
- Recently viewed content

****Advertising Cookies (Optional, with Consent):****

- Interest-based advertising
- Ad performance measurement
- Retargeting and remarketing
- Cross-site tracking (where permitted)

2.4.2 Third-Party Cookies

We allow certain third-party services to set cookies, including:

- Analytics providers (Google Analytics, Mixpanel)
- Advertising networks
- Social media platforms
- Payment processors
- Identity verification services
- Customer support tools

These third parties have their own privacy policies governing their use of your information.

2.4.3 Cookie Management

You can control cookies through:

- **Browser Settings:** Most browsers allow you to refuse cookies or delete existing cookies
- **Cookie Preferences:** Use our cookie preference center (accessible in account settings or footer)
- **Opt-Out Tools:** Industry opt-out tools like the Digital Advertising Alliance or Network Advertising Initiative
- **Do Not Track:** We respond to Do Not Track signals where required by law

Note: Disabling certain cookies may limit platform functionality. Essential cookies cannot be disabled while using the Platform.

2.4.4 Other Tracking Technologies

Web Beacons/Pixels: Small graphic images embedded in emails or web pages to track opens, clicks, and conversions.

Local Storage: HTML5 local storage to store data locally on your device for improved performance and offline functionality.

SDKs and APIs: Third-party software development kits integrated into our mobile applications to provide functionality and collect analytics.

Fingerprinting: We may use device fingerprinting techniques to identify devices for fraud prevention and security purposes.

2.5 Information from Third-Party Sources

We may receive information about you from third-party sources, including:

2.5.1 Identity Verification Services

Third-party verification providers supply:

- Verification results and confidence scores
- Watchlist screening results
- Address verification data
- Identity fraud risk assessments

- Sanctions screening results

2.5.2 Payment Processors

Payment and cryptocurrency service providers share:

- Payment success/failure notifications
- Fraud detection alerts
- Chargeback notifications
- Account verification status
- Transaction confirmation data

2.5.3 Blockchain Data

We collect publicly available blockchain information:

- Transaction history associated with wallet addresses
- Token and NFT ownership records
- Smart contract interaction history
- On-chain identity or reputation scores

2.5.4 Social Media and Public Sources

If you connect social media accounts or if information about you is publicly available:

- Public profile information from connected social accounts
- Publicly available information used for Creator verification
- Public records used for compliance purposes
- Information from data brokers or aggregators (for fraud prevention)

2.5.5 Marketing and Analytics Partners

Marketing partners may provide:

- Attribution data (how you found our Platform)
- Conversion tracking information
- Aggregate demographic data
- Cross-device tracking data (where permitted)

2.5.6 Other Users

Other users may provide information about you:

- When they tag you in content or comments
- When they report your content or account
- When they reference you in communications with us
- When they include you in collaborations or features

2.6 Information We Derive or Infer

Based on the information we collect, we may derive or infer additional information, including:

- ****User Preferences:**** Content preferences, likely interests, predicted behavior
- ****Demographic Information:**** Age range, gender, location (approximate)

- **Device Relationships:** Connecting devices likely used by the same person
 - **Risk Assessments:** Fraud risk scores, account security assessments
 - **Content Recommendations:** Predicted content you may enjoy
 - **Advertising Segments:** Categories for targeted advertising
 - **Engagement Predictions:** Likelihood of subscription renewal, content engagement
 - **Creator Performance Metrics:** Estimated earnings potential, audience demographics
-

3. HOW WE USE YOUR INFORMATION

3.1 Primary Purposes

We use the information we collect for the following purposes:

3.1.1 Providing and Operating the Platform

- **Account Management:** Creating, maintaining, and authenticating your account
- **Service Delivery:** Enabling you to access and use Platform features and functionality
- **Content Delivery:** Displaying, streaming, and delivering content you request
- **Transaction Processing:** Processing purchases, subscriptions, tips, payouts, and other financial transactions
- **Communication:** Facilitating messages between users, sending transactional emails and notifications
- **Customization:** Personalizing your experience based on your preferences and usage patterns
- **Feature Access:** Providing access to features based on your account type and subscription level

3.1.2 Identity Verification and Compliance

- **Age Verification:** Ensuring all users meet minimum age requirements
- **Creator Verification:** Verifying Creator identities and documentation
- **KYC/AML Compliance:** Conducting know-your-customer and anti-money laundering checks
- **Tax Compliance:** Processing tax information, generating tax forms (1099s, etc.)
- **Legal Compliance:** Complying with applicable laws, regulations, and legal obligations
- **Regulatory Reporting:** Reporting to regulatory authorities as required by law
- **Record Keeping:** Maintaining records as required by 18 U.S.C. § 2257 and other regulations

3.1.3 Payment and Financial Services

- **Payment Processing:** Processing cryptocurrency and fiat currency payments
- **Payout Management:** Distributing Creator earnings and managing payout schedules
- **Fee Calculation:** Calculating and collecting platform fees, gas fees, and other charges
- **Financial Reporting:** Generating earnings reports, transaction histories, and account statements
- **Currency Conversion:** Converting between cryptocurrencies and fiat currencies
- **Wallet Integration:** Connecting and managing cryptocurrency wallet integrations
- **NFT Transactions:** Facilitating NFT minting, sales, and transfers
- **Platform Token Management:** Managing Platform Token transactions and utilities

3.1.4 Platform Improvement and Development

- **Analytics:** Analyzing usage patterns, feature performance, and user engagement
- **Product Development:** Developing new features, products, and services
- **Research:** Conducting research to improve our Platform and user experience
- **Testing:** A/B testing, beta testing, and quality assurance
- **Performance Optimization:** Improving loading times, reliability, and efficiency
- **Bug Fixing:** Identifying and resolving technical issues and bugs
- **User Feedback:** Collecting and analyzing user feedback and suggestions

3.1.5 Content Moderation and Safety

- **Content Review:** Reviewing uploaded content for compliance with Terms of Service and Community Guidelines
- **Automated Moderation:** Using automated systems to detect prohibited content
- **User Reports:** Investigating and responding to user reports of violations
- **Account Monitoring:** Monitoring for suspicious activity, fraud, or abuse
- **Prohibited Content Detection:** Detecting and removing illegal or prohibited content (CSAM, non-consensual content, etc.)
- **Community Safety:** Protecting users from harassment, threats, and harmful content
- **DMCA Compliance:** Processing copyright infringement claims and counter-notices

3.1.6 Security and Fraud Prevention

- **Account Security:** Protecting accounts from unauthorized access and takeover
- **Fraud Detection:** Identifying and preventing fraudulent transactions and activities
- **Threat Detection:** Detecting security threats, malware, and malicious activity
- **Access Control:** Enforcing authentication and authorization requirements
- **Security Monitoring:** Monitoring for unusual activity, login patterns, and security incidents
- **Data Protection:** Protecting data from unauthorized access, disclosure, or loss
- **Incident Response:** Responding to security breaches and data incidents

3.1.7 Customer Support

- **Support Services:** Responding to your questions, requests, and issues
- **Technical Assistance:** Providing technical support and troubleshooting
- **Dispute Resolution:** Addressing disputes, complaints, and appeals
- **Account Assistance:** Helping with account recovery, verification issues, and settings
- **Feedback Collection:** Gathering feedback on your experience with support services

3.1.8 Marketing and Communications

- **Promotional Communications:** Sending marketing emails, newsletters, and promotional offers (with your consent where required)
- **Platform Updates:** Notifying you of new features, updates, and changes
- **Creator Opportunities:** Informing Creators of monetization opportunities and programs
- **Event Notifications:** Announcing contests, promotions, and special events
- **Recommendations:** Suggesting content, Creators, or features you may be interested in
- **Engagement:** Encouraging platform engagement and content discovery

3.1.9 Advertising

- **Ad Targeting:** Delivering relevant advertisements based on your interests and behavior
- **Ad Measurement:** Measuring ad performance and effectiveness
- **Retargeting:** Showing ads to users who have visited the Platform

- **Cross-Device Advertising:** Delivering consistent advertising across your devices
- **Third-Party Advertising:** Sharing information with advertising partners (with your consent where required)

3.1.10 Legal and Enforcement

- **Terms Enforcement:** Enforcing our Terms of Service, policies, and agreements
- **Legal Process:** Responding to subpoenas, warrants, court orders, and legal requests
- **Rights Protection:** Protecting our rights, property, and intellectual property
- **Investigations:** Conducting internal investigations of violations or suspicious activity
- **Litigation:** Establishing, exercising, or defending legal claims
- **Law Enforcement Cooperation:** Cooperating with law enforcement agencies

3.1.11 Business Operations

- **Business Analytics:** Analyzing business performance, revenue, and growth metrics
- **Strategic Planning:** Informing business strategy and decision-making
- **Partner Relationships:** Managing relationships with business partners and service providers
- **Mergers and Acquisitions:** Evaluating and executing business transactions
- **Financial Management:** Accounting, auditing, and financial reporting
- **Corporate Governance:** Compliance with corporate policies and procedures

3.2 Legal Bases for Processing (EEA, UK, Switzerland Users)

If you are located in the European Economic Area (EEA), United Kingdom (UK), or Switzerland, we process your personal information based on the following legal grounds:

3.2.1 Contractual Necessity

Processing is necessary to perform our contract with you (the Terms of Service), including:

- Providing access to the Platform
- Processing transactions and payments
- Delivering content and services
- Providing customer support

3.2.2 Legitimate Interests

Processing is necessary for our legitimate interests or those of third parties, including:

- Improving our Platform and services
- Ensuring Platform security and preventing fraud
- Conducting analytics and research
- Marketing our services (where not requiring consent)
- Enforcing our Terms and policies
- Protecting our legal rights

We balance these interests against your rights and freedoms. You have the right to object to processing based on legitimate interests.

3.2.3 Consent

For certain processing activities, we rely on your consent:

- Marketing communications (where required)
- Non-essential cookies and tracking
- Sharing data with certain third parties
- Processing sensitive personal information beyond legal requirements

You may withdraw consent at any time without affecting the lawfulness of processing based on consent before withdrawal.

3.2.4 Legal Obligations

Processing is necessary to comply with our legal obligations:

- Tax reporting and compliance
- AML/KYC requirements
- Response to legal process
- Regulatory reporting
- Record-keeping requirements (18 U.S.C. § 2257)

3.2.5 Vital Interests

In rare cases, processing may be necessary to protect vital interests:

- Preventing harm or danger to individuals
- Emergency situations requiring immediate action

3.3 Automated Decision-Making

We use automated decision-making and profiling in certain circumstances:

3.3.1 Content Recommendations

We use algorithms to recommend content based on your viewing history, preferences, and behavior patterns. You can influence recommendations by adjusting your preferences or clearing your viewing history.

3.3.2 Fraud Detection

We use automated systems to detect fraudulent transactions and suspicious activity. Accounts flagged by these systems may be automatically suspended pending review.

3.3.3 Content Moderation

We use automated tools to detect prohibited content such as CSAM, violence, or copyright infringement. Content flagged by these systems may be automatically removed or restricted.

3.3.4 Risk Assessment

We use automated risk scoring to assess account security, transaction risk, and compliance risk. High-risk transactions may require additional verification.

3.3.5 Your Rights

If you are in the EEA, UK, or Switzerland, you have the right to:

- Obtain human review of automated decisions that significantly affect you
- Express your point of view
- Contest the decision
- Request an explanation of the decision-making logic

To exercise these rights, contact privacy@degencreators.com.

4. HOW WE SHARE YOUR INFORMATION

4.1 Information Sharing Overview

We share your information in the circumstances described below. We do not sell your personal information to third parties for monetary consideration. However, sharing for targeted advertising purposes may constitute a “sale” under certain privacy laws—see Section 8 for more information and opt-out rights.

4.2 Public Information

Certain information is publicly visible on the Platform:

4.2.1 Public Profile Information

- Username and display name
- Profile picture and banner image
- Bio and description
- Social media links
- Public content posts (not behind paywalls)
- Subscriber counts (if not hidden in settings)
- Account creation date
- Creator verification badges

4.2.2 Public Content

- Content not restricted to subscribers
- Public comments and interactions
- Public ratings and reviews
- Content shared outside the Platform by you

4.2.3 Blockchain Information

- Wallet addresses you use
- NFT ownership and transactions
- Platform Token transactions
- Smart contract interactions
- All blockchain data is permanently public and visible to anyone

****Privacy Controls:**** You can adjust privacy settings to control what information is publicly visible, though some information (username, public content) must remain public for the Platform to function.

4.3 With Other Users

We share information with other users as necessary for Platform functionality:

4.3.1 Creator-Subscriber Interactions

- Your username and profile information with Creators you subscribe to
- Your messages and interactions with Creators
- Your subscription status and tier
- Your tipping and purchase history (with the specific Creator)

4.3.2 Subscriber Information to Creators

Creators can see limited information about their subscribers:

- Usernames of subscribers
- Subscription dates and status
- Subscription tier
- Aggregated subscriber demographics (no personally identifiable information)
- Interaction history (views, likes, comments)

Creators cannot see:

- Your email address (unless you provide it in messages)
- Your payment method details
- Your full transaction history
- Other subscriptions or purchases
- Your private account information

4.3.3 Comments and Public Interactions

Public comments, likes, and interactions are visible to other users as part of the Platform's social features.

4.4 Service Providers and Business Partners

We share information with third-party service providers who perform services on our behalf:

4.4.1 Infrastructure and Hosting

- Cloud hosting providers (AWS, Google Cloud, etc.)
- Content delivery networks (CDNs)
- Database and storage providers
- Server management and monitoring services

These providers have access to your data only as necessary to perform their functions and are obligated to protect it.

4.4.2 Payment Processors

- Credit card and payment processors
- Cryptocurrency payment processors
- Bank transfer services
- Payout and remittance providers
- Tax reporting services

Payment processors collect and process payment information according to their own privacy policies. We do not control their data practices.

4.4.3 Identity Verification

- KYC/AML verification services
- Document verification providers
- Biometric verification services
- Fraud detection services
- Background check providers (where applicable)

These services receive identity documents and personal information necessary for verification purposes.

4.4.4 Analytics and Research

- Usage analytics platforms (Google Analytics, Mixpanel, etc.)
- A/B testing services
- User research and survey platforms
- Heat mapping and session recording tools

These services help us understand how users interact with the Platform.

4.4.5 Marketing and Advertising

- Email marketing platforms
- Advertising networks and exchanges
- Social media advertising platforms
- Retargeting and remarketing services
- Attribution and conversion tracking services

We share information necessary to deliver, measure, and optimize advertising.

4.4.6 Customer Support

- Customer support and helpdesk platforms
- Live chat providers
- Ticketing systems
- Communication tools

Support providers have access to your communications and account information necessary to assist you.

4.4.7 Security and Fraud Prevention

- Fraud detection and prevention services
- DDoS protection services
- Bot detection services
- Security monitoring tools
- Threat intelligence providers

These services help protect the Platform and users from security threats.

4.4.8 Blockchain and NFT Services

- Blockchain node providers
- IPFS pinning services
- NFT metadata storage providers
- Smart contract platforms
- Decentralized storage networks

These providers facilitate blockchain and NFT functionality.

4.4.9 Other Service Providers

- Legal and professional advisors
- Auditors and accountants
- Insurance providers
- Business consultants
- Translation services
- Communication platforms

4.5 Business Transfers

In the event of a merger, acquisition, reorganization, bankruptcy, or sale of assets:

- We may transfer your information to the successor entity
- Your information remains subject to privacy commitments
- You will be notified of any material changes to information handling
- You may have the right to object or delete your account before the transfer

4.6 Legal Requirements and Protection of Rights

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

4.6.1 Comply with Legal Obligations

- Respond to subpoenas, warrants, or court orders
- Comply with applicable laws and regulations
- Respond to lawful requests from government authorities
- Meet tax reporting and regulatory requirements
- Fulfill record-keeping obligations

4.6.2 Protect Rights and Safety

- Enforce our Terms of Service and policies
- Protect our rights, property, and intellectual property
- Investigate fraud, security issues, or Terms violations
- Protect the safety of users and the public
- Prevent illegal activity or harm
- Establish, exercise, or defend legal claims

4.6.3 Law Enforcement Cooperation

- Report suspected illegal activity (CSAM, trafficking, etc.)
- Cooperate with law enforcement investigations
- Provide evidence in criminal or civil proceedings

- Comply with national security requests (where legally required)

We will notify you of legal requests for your information unless prohibited by law or court order.

4.7 With Your Consent

We may share your information with third parties when you provide specific consent, including:

- Connecting third-party services to your account
- Participating in surveys or research studies
- Entering contests or promotions with third-party partners
- Authorizing specific data sharing

You can revoke consent at any time where technically feasible.

4.8 Aggregated and De-Identified Information

We may share aggregated, de-identified, or anonymous information that does not identify you personally:

- Platform usage statistics and trends
- Demographic information about our user base
- Content performance metrics
- Industry research and reports
- Business performance indicators

This information cannot reasonably be used to identify you and is not subject to this Privacy Policy's restrictions.

4.9 Information Sharing Limitations

We do not share your information with third parties for their independent marketing purposes without your consent, except as required by law or as described in this Privacy Policy.

Service providers are contractually required to:

- Use your information only for specified purposes
- Implement appropriate security measures
- Comply with applicable data protection laws
- Delete or return information when services are complete
- Not use information for their own purposes

5. DATA RETENTION

5.1 Retention Periods

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

5.1.1 Active Accounts

While your account is active:

- We retain account information, profile data, and preferences
- Content you upload is retained and accessible
- Transaction history and financial records are maintained
- Communications and messages are stored
- Usage data and logs are retained according to our retention schedule

5.1.2 Inactive Accounts

For inactive accounts (no login for extended period):

- We may send reminders before taking action
- After [time period], we may deactivate the account
- After [longer time period], we may delete the account and associated data
- You can reactivate your account before deletion by logging in

5.1.3 Deleted Accounts

When you delete your account:

- Account access is immediately terminated
- Most data is deleted within 90 days
- Some data is retained for legal, security, or business purposes (see below)
- Blockchain data cannot be deleted (it is permanent and public)
- Backups containing your data may persist for up to 180 days

5.1.4 Specific Data Types

****Identity Verification Documents:****

- Retained for the duration of your account plus 7 years to comply with legal requirements
- May be retained longer if required by law or ongoing legal proceedings

****Financial and Tax Records:****

- Retained for 7 years to comply with tax laws and regulations
- Transaction records retained for accounting and audit purposes
- Payout history retained to resolve disputes

****Content:****

- Creator Content is deleted when you delete it or your account (subject to backup retention)
- Content may be retained if subject to legal hold or ongoing investigation
- Metadata may be retained for analytics purposes

****Communications:****

- Customer support communications retained for 3 years
- Direct messages may be deleted with your account
- Reported content and associated communications retained for enforcement purposes

****Usage Data and Logs:****

- Server logs retained for 90 days for security and troubleshooting

- Analytics data retained for 26 months
- Aggregated or de-identified data may be retained indefinitely

****Blockchain Data:****

- Blockchain transactions are permanent and cannot be deleted
- NFT metadata stored on decentralized networks may persist indefinitely
- We have no control over blockchain data retention

****Legal Hold Data:****

- Data subject to legal holds, investigations, or litigation is retained until the matter is resolved
- We will notify you if your data is subject to a legal hold

5.2 Retention Criteria

We determine retention periods based on:

- The nature and sensitivity of the information
- The purposes for which we collected it
- Legal, regulatory, tax, and accounting requirements
- Statute of limitations for potential legal claims
- Business operational needs
- User expectations and requests
- Industry best practices

5.3 Secure Deletion

When we delete your information:

- Data is permanently removed from active systems
- Backups are overwritten according to backup retention schedules
- Secure deletion methods prevent recovery
- Service providers are instructed to delete data
- Some residual data may persist in systems for technical reasons

We cannot delete:

- Information required to be retained by law
- Information necessary for ongoing legal proceedings
- Blockchain data (permanent and public)
- Aggregated or de-identified information

6. DATA SECURITY

6.1 Security Measures

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

6.1.1 Technical Security

****Encryption:****

- TLS/SSL encryption for data in transit
- Encryption at rest for sensitive data
- Encrypted backups
- Encrypted database connections
- End-to-end encryption for certain communications

****Access Controls:****

- Multi-factor authentication for employee access
- Role-based access control (RBAC)
- Principle of least privilege
- Regular access reviews and audits
- Automatic session timeouts

****Network Security:****

- Firewalls and intrusion detection systems
- DDoS protection and mitigation
- Network segmentation
- Regular vulnerability scanning
- Penetration testing

****Application Security:****

- Secure coding practices
- Regular security updates and patches
- Input validation and sanitization
- Protection against common attacks (SQL injection, XSS, CSRF)
- Security testing in development lifecycle

****Authentication:****

- Strong password requirements
- Password hashing (bcrypt or similar)
- Two-factor authentication options
- Account lockout after failed attempts
- Suspicious login detection

6.1.2 Administrative Security

****Policies and Procedures:****

- Information security policies
- Incident response procedures
- Data classification standards
- Acceptable use policies
- Vendor management procedures

****Employee Training:****

- Security awareness training
- Privacy and data protection training

- Social engineering awareness
- Regular security updates and reminders
- Confidentiality agreements

****Access Management:****

- Background checks for employees with data access
- Secure onboarding and offboarding procedures
- Regular review of employee access rights
- Immediate revocation of access for terminated employees

****Vendor Management:****

- Security assessments of third-party vendors
- Contractual security and privacy requirements
- Regular vendor audits and reviews
- Data processing agreements

6.1.3 Physical Security

****Data Centers:****

- Secure, access-controlled facilities
- 24/7 monitoring and security personnel
- Redundant power and cooling systems
- Fire suppression and disaster protection
- Compliance certifications (SOC 2, ISO 27001, etc.)

****Office Security:****

- Restricted access to facilities
- Visitor logging and escort requirements
- Secure disposal of physical documents
- Device encryption and remote wipe capabilities

6.1.4 Monitoring and Response

****Security Monitoring:****

- 24/7 security monitoring and logging
- Real-time threat detection
- Automated security alerts
- Regular log review and analysis
- Anomaly detection systems

****Incident Response:****

- Dedicated incident response team
- Incident response plan and procedures
- Regular incident response drills
- Forensic investigation capabilities
- Notification procedures for breaches

****Vulnerability Management:****

- Regular vulnerability assessments
- Patch management program
- Security update procedures
- Bug bounty program
- Third-party security audits

6.2 Your Security Responsibilities

You play a crucial role in protecting your account:

****Account Security:****

- Choose a strong, unique password
- Enable two-factor authentication
- Never share your password or 2FA codes
- Log out when using shared devices
- Keep your email account secure
- Review account activity regularly

****Device Security:****

- Keep your devices and software updated
- Use antivirus/anti-malware software
- Secure your devices with passwords/biometrics
- Be cautious of public Wi-Fi
- Don't root/jailbreak devices used for sensitive transactions

****Phishing Awareness:****

- Be suspicious of unsolicited communications
- Verify sender authenticity before clicking links
- Don't provide sensitive information via email
- Report suspected phishing to security@degencreators.com
- We will never ask for your password via email

****Wallet Security:****

- Protect your private keys and seed phrases
- Never share private keys with anyone
- Use hardware wallets for significant holdings
- Verify recipient addresses before sending crypto
- Be cautious of wallet connection requests

****Reporting:****

- Immediately report suspected unauthorized access
- Report suspicious activity or security vulnerabilities
- Contact security@degencreators.com for security concerns

6.3 Limitations of Security

Despite our security measures, no system is completely secure:

****Risks:****

- Sophisticated cyberattacks may breach defenses
- User error can compromise security
- Third-party vulnerabilities may affect our security
- Blockchain transactions are irreversible
- Lost private keys cannot be recovered

****No Guarantee:****

- We cannot guarantee absolute security
- Unauthorized access may occur despite our efforts
- You assume inherent risks when using the Platform
- You are responsible for your own security practices

6.4 Data Breach Response

In the event of a data breach:

****Investigation:****

- We will promptly investigate the incident
- Determine the scope and impact of the breach
- Identify affected users and data
- Assess risks to affected individuals

****Notification:****

- Notify affected users without undue delay
- Provide information about the breach
- Advise on steps to protect yourself
- Offer assistance (credit monitoring, etc.) where appropriate

****Remediation:****

- Take steps to contain and remediate the breach
- Implement additional security measures
- Review and improve security practices
- Cooperate with law enforcement

****Compliance:****

- Comply with all applicable breach notification laws
- Notify regulators as required
- Maintain records of the incident
- Report to relevant authorities

To report a security vulnerability: security@degencreators.com

7. INTERNATIONAL DATA TRANSFERS

7.1 Cross-Border Transfers

DegenCreators is based in the United States, and our servers and service providers may be located in various countries worldwide. By using the Platform, you acknowledge that your information may be transferred to, stored in, and processed in countries other than your own.

7.1.1 Transfers from the EEA, UK, and Switzerland

If you are located in the European Economic Area (EEA), United Kingdom (UK), or Switzerland, your personal information may be transferred to countries that do not provide the same level of data protection as your home country.

We implement appropriate safeguards for these transfers:

****Standard Contractual Clauses (SCCs):****

- We use European Commission-approved Standard Contractual Clauses
- SCCs provide contractual guarantees for data protection
- Available upon request

****Adequacy Decisions:****

- We transfer data to countries deemed adequate by the European Commission
- Currently includes Switzerland, Canada, Japan, and others

****Additional Safeguards:****

- Supplementary measures beyond SCCs where necessary
- Technical and organizational measures
- Encryption and pseudonymization
- Regular assessment of transfer risks

7.1.2 Transfers to the United States

Data transferred to the United States is subject to:

- U.S. privacy laws and regulations
- Potential access by U.S. government agencies
- Different legal protections than EEA/UK laws
- Standard Contractual Clauses for protection

The United States does not currently have an adequacy decision from the European Commission. We rely on SCCs and additional safeguards to protect your data.

7.1.3 Other International Transfers

We may transfer data to other countries based on:

- Standard Contractual Clauses
- Adequacy decisions
- Your explicit consent
- Necessity for contract performance
- Other legal transfer mechanisms

7.2 Blockchain Considerations

Blockchain data is inherently global and decentralized:

- Cannot be restricted to specific jurisdictions
- Visible worldwide to anyone with internet access
- Cannot be deleted or restricted after recording
- Subject to varying laws in different countries

By engaging in blockchain transactions, you acknowledge this global nature.

7.3 Your Rights Regarding Transfers

If you are in the EEA, UK, or Switzerland:

- You may request information about transfer safeguards
- You may request copies of Standard Contractual Clauses
- You may object to transfers in certain circumstances
- You may lodge complaints with supervisory authorities

Contact privacy@degencreators.com for information about data transfers.

8. YOUR PRIVACY RIGHTS AND CHOICES

8.1 General Rights

Depending on your location, you may have the following rights regarding your personal information:

8.1.1 Access and Portability

****Right to Access:****

- Request confirmation of whether we process your personal information
- Obtain a copy of your personal information
- Receive information about how we use your data

****Right to Data Portability:****

- Receive your data in a structured, machine-readable format
- Transmit your data to another service provider
- Applies to data you provided and that we process automatically

To exercise these rights, use the data download feature in your account settings or contact privacy@degencreators.com.

8.1.2 Correction and Update

****Right to Correction:****

- Correct inaccurate personal information
- Complete incomplete personal information

- Update outdated information

You can update most information directly in your account settings. For other corrections, contact privacy@degencreators.com.

8.1.3 Deletion and Erasure

****Right to Deletion (“Right to be Forgotten”):****

- Request deletion of your personal information
- Applies when information is no longer necessary
- Applies when you withdraw consent or object to processing

****Limitations:****

- We may retain data required by law
- We may retain data necessary for legal claims
- Blockchain data cannot be deleted
- Aggregated or de-identified data may be retained

To delete your account and data: Use account settings or contact privacy@degencreators.com.

8.1.4 Restriction and Objection

****Right to Restriction:****

- Limit how we use your personal information
- While accuracy is being verified
- When processing is unlawful but you prefer restriction over deletion

****Right to Object:****

- Object to processing based on legitimate interests
- Object to direct marketing (absolute right)
- Object to automated decision-making and profiling

To exercise these rights, contact privacy@degencreators.com.

8.2 Specific Rights by Jurisdiction

8.2.1 European Economic Area, UK, and Switzerland

Under GDPR and similar laws, you have:

- All rights listed in Section 8.1
- Right to lodge a complaint with supervisory authority
- Right to effective judicial remedy
- Right not to be subject to automated decision-making
- Right to withdraw consent at any time
- Right to object to processing for direct marketing

****Supervisory Authorities:****

- EEA: Your local Data Protection Authority

- UK: Information Commissioner's Office (ICO)
- Switzerland: Federal Data Protection and Information Commissioner (FDPIC)

8.2.2 California Residents (CCPA/CPRA)

Under the California Consumer Privacy Act and California Privacy Rights Act, you have:

****Right to Know:****

- Categories of personal information collected
- Categories of sources
- Business purposes for collection
- Categories of third parties we share with
- Specific pieces of personal information

****Right to Delete:****

- Request deletion of personal information
- Subject to exceptions for legal compliance, fraud prevention, etc.

****Right to Opt-Out:****

- Opt out of “sale” or “sharing” of personal information
- We do not sell personal information for money
- Sharing for targeted advertising may constitute a “sale”
- Use “Do Not Sell or Share My Personal Information” link in footer

****Right to Correct:****

- Correct inaccurate personal information

****Right to Limit:****

- Limit use of sensitive personal information
- Applies to use beyond what’s necessary for services

****Right to Non-Discrimination:****

- We will not discriminate for exercising your rights
- Same service quality and pricing

****Authorized Agents:****

- You may designate an authorized agent to make requests
- Agent must provide proof of authorization

****Shine the Light:****

- Annual request for disclosure of information shared with third parties for marketing

To exercise CCPA/CPRA rights:

- Email: privacy@degencreators.com
- Phone: [Phone Number]

- Online form: [URL]

We will verify your identity before processing requests.

8.2.3 Other U.S. State Privacy Laws

If you reside in Virginia, Colorado, Connecticut, Utah, or other states with comprehensive privacy laws, you may have similar rights to those under CCPA/CPRA:

- Right to access personal information
- Right to correct inaccuracies
- Right to delete personal information
- Right to opt out of targeted advertising
- Right to opt out of profiling
- Right to opt out of sales of personal information

Contact privacy@degencreators.com to exercise these rights.

8.2.4 Other Jurisdictions

Users in other jurisdictions may have rights under applicable local laws. Contact privacy@degencreators.com for information about your specific rights.

8.3 Marketing and Communications Preferences

Email Marketing:

- Opt out using unsubscribe links in marketing emails
- Adjust preferences in account settings
- [Email preferences@degencreators.com](mailto:Email%20preferences@degencreators.com)

Push Notifications:

- Manage through device settings
- Manage through app notification settings

SMS Marketing:

- Reply STOP to opt-out messages
- Manage in account settings

Transactional Communications:

- Cannot opt out of essential transactional emails
- These include security alerts, legal notices, transaction confirmations

8.4 Cookie and Tracking Preferences

Cookie Management:

- Use our Cookie Preference Center (footer/settings)
- Adjust browser cookie settings
- Use third-party opt-out tools

****Do Not Track:****

- We respond to Do Not Track signals where required by law
- Browser DNT settings may affect tracking

****Targeted Advertising Opt-Out:****

- Opt out via Digital Advertising Alliance: [URL]
- Opt out via Network Advertising Initiative: [URL]
- Opt out via Your Online Choices (EU): [URL]
- Platform-specific opt-outs (Google, Facebook, etc.)

****Mobile Advertising:****

- iOS: Limit Ad Tracking in device settings
- Android: Opt out of Ads Personalization in device settings

8.5 Account Closure and Deletion

****Close Your Account:****

- Go to Account Settings > Close Account
- Follow the deletion process
- Email privacy@degencreators.com if you need assistance

****What Happens:****

- Immediate access termination
- Content deletion within 90 days
- Some data retained for legal/business purposes
- Blockchain data cannot be deleted

****Before Closing:****

- Download your data
- Withdraw any pending payments
- Cancel active subscriptions
- Backup important information

8.6 Exercising Your Rights

****How to Make Requests:****

- Email: privacy@degencreators.com
- Online Form: [URL]
- Mail: DegenCreators, LLC, Attn: Privacy Officer, [Address]

****Information to Include:****

- Your name and contact information
- Username and account email
- Specific right(s) you wish to exercise
- Sufficient detail to locate your information

****Verification:****

- We will verify your identity before fulfilling requests
- May request additional information for verification
- May use two-factor authentication or other methods

****Response Time:****

- We will respond within 30 days (45 days if complex)
- May extend by additional 30 days with notice
- Will inform you if we cannot fulfill your request

****No Fee:****

- We do not charge fees for requests
- May charge reasonable fee for excessive or repetitive requests
- May refuse manifestly unfounded requests

****Appeals:****

- If we deny your request, you may appeal
- Email appeals to privacy@degencreators.com
- Include request details and reason for appeal
- We will respond within 30 days

9. CHILDREN'S PRIVACY

9.1 Age Restrictions

The Platform is not intended for, and we do not knowingly collect information from, anyone under the age of 18.

****Our Policy:****

- We require all users to be at least 18 years old
- We implement age verification mechanisms
- We do not knowingly collect data from minors
- We prohibit all content involving minors

9.2 Parental Notice

If you are a parent or guardian and believe your child under 18 has provided information to us:

- Contact us immediately at privacy@degencreators.com
- Provide your child's username and any relevant information
- We will promptly investigate and delete the account
- We will delete all associated information

9.3 What We Do When We Learn of Underage Users

If we discover or are notified that a user is under 18:

- Immediately terminate the account
- Delete all associated content and information
- Remove all personally identifiable information
- Report to authorities if required by law
- Investigate how the user bypassed age verification
- Strengthen age verification if necessary

9.4 Compliance with COPPA

Although the Platform is not directed to children under 13, we comply with the Children's Online Privacy Protection Act (COPPA):

- We do not knowingly collect information from children under 13
- We do not condition participation on disclosure of more information than necessary
- We respond to parental requests to review or delete children's information
- We maintain reasonable security for children's information

9.5 Report Suspected Underage Users

If you suspect a user is under 18:

- Report immediately to abuse@degencreators.com
- Provide username and supporting evidence
- Do not interact with the suspected minor
- We will investigate promptly

10. THIRD-PARTY SERVICES AND LINKS

10.1 Third-Party Websites and Services

The Platform may contain links to third-party websites, services, or applications:

****Our Responsibility:****

- We are not responsible for third-party privacy practices
- We do not control third-party content or policies
- Links do not imply endorsement
- We encourage you to read third-party privacy policies

****Your Responsibility:****

- Review privacy policies before providing information
- Understand data practices of third-party services
- Make informed decisions about data sharing

10.2 Social Media Platforms

If you connect social media accounts:

****Information Shared:****

- Profile information from your social account

- Friends/followers who also use our Platform
- Posts or activity you choose to share

****Control:****

- Review social media platform privacy settings
- Disconnect at any time through account settings
- Social platforms may continue to collect information

****Social Sharing:****

- You may share content to social media
- Subject to social platform terms and privacy policies
- Shared content becomes subject to social platform rules

10.3 Payment Processors

Third-party payment processors (Stripe, PayPal, cryptocurrency processors) collect and process payment information:

****Their Practices:****

- Governed by their own privacy policies
- May use information for fraud prevention
- May retain information per their policies

****Our Access:****

- We receive limited payment information
- We do not store full credit card numbers
- We do not control payment processor practices

10.4 Identity Verification Services

Third-party verification providers process identity documents:

****Information Shared:****

- Government-issued IDs
- Biometric data
- Verification results

****Their Use:****

- Verification and fraud prevention
- Compliance with their regulatory obligations
- Governed by their privacy policies

10.5 Analytics and Advertising Services

Third-party analytics and advertising services:

****Services We Use:****

- Google Analytics
- Facebook Pixel
- Advertising networks
- Attribution services

****Their Practices:****

- Collect information through cookies and tags
- May build profiles across websites
- Subject to their own privacy policies

****Your Control:****

- Opt out through service-specific mechanisms
- Use browser privacy settings
- Use our cookie preference center

10.6 Blockchain and Decentralized Services

Blockchain networks and decentralized services:

****Nature:****

- Operate independently of DegenCreators
- Information is publicly visible and permanent
- No central authority controls data

****Our Role:****

- We facilitate access to these services
- We do not control blockchain data
- We cannot delete blockchain information

****Your Understanding:****

- Blockchain transactions are permanent
- Wallet addresses are pseudonymous but not anonymous
- Anyone can view blockchain data

11. CALIFORNIA SHINE THE LIGHT LAW

California Civil Code Section 1798.83 permits California residents to request information about disclosure of personal information to third parties for direct marketing purposes.

****Your Rights:****

- Request information once per calendar year
- Receive categories of personal information shared
- Receive names and addresses of third parties

****Our Practice:****

- We do not share personal information with third parties for their direct marketing purposes
- If our practices change, we will update this policy
- We will honor Shine the Light requests

****How to Request:****

- Email: privacy@degencreators.com
- Subject: "California Shine the Light Request"
- Include your name, address, and username

12. NEVADA PRIVACY RIGHTS

Nevada residents have the right to opt out of the sale of certain personal information.

****Our Practice:****

- We do not currently sell personal information as defined by Nevada law
- If our practices change, we will provide opt-out mechanisms
- We will honor Nevada opt-out requests

****How to Opt Out:****

- Email: privacy@degencreators.com
- Subject: "Nevada Do Not Sell Request"
- Include your name and username

13. CHANGES TO THIS PRIVACY POLICY

13.1 Right to Modify

We reserve the right to modify this Privacy Policy at any time to reflect:

- Changes in our data practices
- New features or services
- Legal or regulatory requirements
- Technological developments
- Business changes

13.2 Notice of Changes

When we make material changes:

****Notification Methods:****

- Update "Last Updated" date
- Post revised policy on the Platform
- Email notice to registered users
- Display prominent notice on the Platform
- Provide 30 days' notice before changes take effect (where required)

****Minor Changes:****

- May be made without notice
- Reflected in updated “Last Updated” date
- Check periodically for updates

13.3 Your Acceptance

****Continued Use:****

- Continued use after changes constitutes acceptance
- If you disagree, stop using the Platform
- You may delete your account if you don’t accept changes

****Material Changes:****

- May require affirmative consent in some cases
- You will be prompted to accept updated policy
- Failure to accept may limit access to Platform

13.4 Version History

Previous versions of this Privacy Policy are available upon request:

- Email: privacy@degencreators.com
- Subject: “Privacy Policy Version Request”
- Specify which version you need

14. CONTACT US

14.1 Privacy Questions and Requests

For privacy-related questions, concerns, or requests:

****General Privacy:****

Email: privacy@degencreators.com
Mail: DegenCreators, LLC, Attn: Privacy Officer, [Address]

****Data Subject Requests:****

Online Form: [URL]
Email: privacy@degencreators.com

****Security Concerns:****

Email: security@degencreators.com

****Data Protection Officer (EEA/UK/Switzerland):****

Email: dpo@degencreators.com

14.2 Supervisory Authorities

****EEA Residents:****

Contact your local Data Protection Authority. List available at: <https://edpb.europa.eu/about-edpb/board/members_en>

****UK Residents:****

Information Commissioner's Office (ICO)

Website: <<https://ico.org.uk>>

Phone: 0303 123 1113

****Swiss Residents:****

Federal Data Protection and Information Commissioner (FDPIC)

Website: <<https://www.edoeb.admin.ch>>

Email: info@edoeb.admin.ch

14.3 Response Time

We will respond to your inquiries:

- Within 30 days for most requests
- Within 45 days for complex requests
- Within timeframes required by applicable law
- We will inform you if we need more time

****DegenCreators, LLC****

****Last Updated: January 18, 2026****

****Version 1.0****

****End of Privacy Policy****