PRIVACY POLICY
CRIPCOM (APP / WEB)
vs.001 — SEALED (EN)

Data Controller: CripCom Trade LLC (USA)
Sealing date: 05-Mar-2026

STATUS	SEALED VERSION (vs.001)
SEALED VERSION	vs.001
DATE	05-Mar-2026
DOCUMENT OWNER	LDO (LEGAL DOCUMENT OFFICER)
APPROVER (SPONSOR)	CLO (CHIEF LEGAL OFFICER)
DATA CONTROLLER	CripCom Trade LLC (USA)
SCOPE	USA + global alignment (LATAM, Spain, Italy, Israel, Germany, UAE, UK).
CHANNELS	Web, App, email, social media, WhatsApp (support/communications), chats; Telegram (future).
MAIN PROCESSORS	Didit (KYC), Stripe (payments), AWS (infrastructure), Google Workspace, Amplitude (analytics).
RETENTION (SSOT)	Active account + minimum 5 years (longer if required by law or dispute).
RULES	No sale of data. Marketing with opt-out. Biometrics only for verification/fraud/compliance.

Sealing clause (SSOT)

This Privacy Policy is sealed as version vs.001. Any subsequent modification must follow the applicable Change & Sealing Protocol and will create a new version.

1. Who we are, scope and language

CripCom Trade LLC ("CripCom", "we", "us") is the data controller responsible for the processing described in this Policy. This Policy applies to CripCom's App, website, official communications and official channels.

This Policy explains what personal data we collect, how we use it, who we share it with, how long we retain it, how we protect it, and what rights you may have. It applies to users in the USA and international users, without prejudice to mandatory rights under applicable laws.

Language & precedence: this Policy may be available in English and Spanish. For relationships and users subject to the United States and/or where English is the applicable language, the English version may prevail. For Spanish-speaking users, the Spanish version is provided as a main reference. In case of discrepancy, the version indicated by CripCom according to the applicable jurisdiction will apply, to the extent permitted by law.

2. Personal data we collect and sources

Category	Examples	Source
Identification & contact	First/last name, email, phone	User
Identity (KYC)	ID document, selfie, biometrics	User + Didit
Residence/location	Address, city, country	User
Payments	Minimal billing data, transaction IDs/status	User + Stripe
Support	Chats, tickets, messages, attachments	User + official channels
Usage/analytics	Usage events, metrics, technical identifiers	App/Web + Amplitude
Marketing	Preferences, consent and opt-out	User + channels

We do not request private keys. We will never ask for your password or authentication codes through non-official channels.

3. Purposes and legal bases (global framework)

We use personal data to operate the Platform, verify identity, process payments, provide support, improve the service, prevent fraud, comply with legal obligations and communicate with you.

Purpose	Typical data	Legal basis (framework)
Operate account/App/Web	Contact, usage/analytics, support	Contract performance (Terms)
KYC/AML and security	KYC/biometrics, residence, risk signals	Legal obligation / legitimate interests / consent where applicable
Payments and disputes	Minimal billing, transactions, support	Contract performance / payment obligations
Fraud prevention	Usage, technical signals, KYC/payments	Legitimate interests / compliance
Product improvement	Analytics events (Amplitude)	Legitimate interests (minimization)
Marketing	Contact, preferences	Consent where applicable + opt-out

4. KYC, biometrics, fraud prevention and acceptance logs

We may require identity verification (KYC) to enable or maintain certain features. This may include ID documents, selfies and biometric checks. Biometrics may be considered sensitive data in some jurisdictions: it is used only for verification, fraud prevention and compliance; it is not used for marketing.

We may use automated tools for fraud prevention, KYC or security. If an automated decision has significant effects (e.g., full blocking), we provide a human review channel via support, subject to security, fraud and compliance constraints.

CripCom may collect and retain technical logs such as IP address, date/time, session/device identifiers and security events for security, fraud prevention, auditability and evidence of acceptance of Terms and Policies.

5. Payments (Stripe) and financial data

We use Stripe as a payment processor. Stripe processes payment instruments; CripCom does not store full card numbers. We may retain transaction IDs/status and minimal billing data where applicable, and use such data to resolve disputes/chargebacks and for fraud prevention.

CripCom operates corporate bank accounts (e.g., Chase, Citi, Banesco Panama). By default, we do not collect full user bank account details for Stripe card payments. If bank transfers are enabled in the future, this Policy will be updated.

6. Service providers, international transfers and no sale of data

We share data with processors necessary to operate the Platform. Given global operations, your data may be transferred and processed outside your country, including the United States. Where required by law, we apply reasonable safeguards (e.g., contractual arrangements and organizational measures) to protect data.

Processor	Role	Purpose	Typical data
Didit	Processor (KYC)	Identity verification	ID, selfie/biometrics, identity
Stripe	Processor (payments)	Payments and disputes	Minimal billing, payment IDs/status
AWS	Processor (infrastructure)	Hosting/operations	Operational account/service data
Google Workspace	Processor (tools)	Email/internal tools	Communications and internal support
Amplitude	Processor (analytics)	Measurement and improvement	Usage events and technical IDs

We do not sell personal data. We share data only to operate the Platform, comply with law, prevent fraud, or with your consent where applicable.

7. Retention and deletion

SSOT rule: we retain data while your account is active and for a minimum of 5 years thereafter. We may retain longer if required by law, if there is an investigation/dispute/claim, or if reasonably necessary for fraud prevention and legal defense.

After retention periods, we delete or anonymize data. Some data may remain temporarily in backups for technical reasons and will be deleted according to backup cycles.

Analytics (Amplitude): target retention of events is 24 months (or the minimum equivalent configured), with a minimization approach and, where applicable, anonymization or pseudonymization of identifiers.

8. Security

- Access controls (least privilege) and credential management.
- Encryption in transit (TLS) and, where applicable, at rest.
- Monitoring and logging for incident detection.

- Contractual requirements and reasonable security standards applicable to critical suppliers (e.g., Didit, Stripe, AWS and Google).

No system is 100% secure. You are also responsible for protecting your credentials and devices.

9. Marketing, cookies and communications

Marketing: you can opt out at any time: (i) email: unsubscribe link in each promotional email; (ii) WhatsApp: replying “STOP” or requesting removal via an official channel; (iii) in-app preferences if available. Even after opting out of marketing, CripCom may continue to send necessary transactional, operational or legal communications (e.g., security, material changes, confirmations and support).

Cookies and similar technologies on the website are additionally governed by Annex PP-A — Cookies Notice and Consent. CripCom may currently operate the website without non-essential cookies. If analytics or marketing cookies are introduced in the future, CripCom will implement a consent notice/manager for cookies that are not strictly necessary, according to the applicable jurisdiction. Strictly necessary cookies may operate without consent where permitted by law.

Social media and external links: interactions on social platforms are governed by the relevant platform policies.

10. Rights, minors, contact and notices

Depending on your jurisdiction, you may have rights such as access, rectification, deletion, objection, restriction, portability and withdrawal of consent, where applicable. We may require identity verification and may limit requests where necessary for legal compliance, fraud prevention or legal defense.

Target response time (SLA): CripCom will respond to privacy requests within the period applicable under the relevant jurisdiction. As an internal operational reference, the target response time will be up to 30 calendar days from receipt of the request. In complex cases or where permitted by law, that period may be extended; in such case, CripCom will inform the user.

Minors / Youth Mode. As a general rule, the Platform is not intended for minors. However, CripCom may enable an educational mode for minors (“Youth Mode”) only under the supervision and responsibility of a parent/legal guardian (“Guardian”) and pursuant to the then-current Minors (Youth Mode) Public Policy. In Youth Mode: (i) the minor cannot make purchases/payments/withdrawals or conduct direct financial transactions; (ii) CripCom minimizes the minor’s data and does not conduct direct marketing to the minor; and (iii) the Guardian may exercise privacy rights on the minor’s behalf where applicable. CripCom may require Guardian verification and, where required by law, verifiable parental consent.

Privacy contact: privacy@cripcomft.com. Support contact: soporte@cripcomft.com.

Legal notices (domicile): CripCom Trade LLC — Attn: Legal Notices — c/o Registered Agent (per current corporate filing in the US state of organization).

11. Updates to this Policy

We may update this Policy. If changes are material, we will notify you through reasonable means (in-app or email) and may request renewed acceptance where appropriate. The current version will be the one published through official channels.