AML / CFT Policy

Version 1.0 | Updated 11 November 2026
clirizo.com | info@clirizo.com

1. Purpose and accountability

Clirizo uses this Policy to define safeguards against money laundering, terrorist financing, proliferation financing, sanctions circumvention and related fraud. It covers customers, applicants and personnel involved in services accessible through clirizo.com. FATF risk-based principles inform the approach, with enforceable duties determined by the applicable legal framework. Live activity requires suitable procedures, competent compliance personnel and clear responsibility for escalation and statutory reporting.

2. KYC/KYB before a relationship

Successful completion of the applicable Know Your Customer or Know Your Business procedure is a prerequisite to every business relationship with Clirizo. Submission of a form is a preliminary request for review. Checks must identify the applicant, legitimate activity, authorised representatives and the individuals ultimately controlling the business. Reliable and independent sources support verification. Unverified, fictitious or anonymous parties cannot be accepted into a business relationship.

3. Evidence and risk classification

Collect proportionate identity information and independent evidence for individuals. For businesses, verify registration, operating locations, controllers, directors and representative authority, applying local ownership rules. Classify risk by activity, customer characteristics, geography, expected volumes, delivery method and counterparties. Reviews must respond to changed circumstances and the assigned risk. Reduced checks require a permitted low-risk basis and must never replace investigation where suspicious circumstances exist.

4. Sanctions and geographic eligibility

Eligibility depends on sanctions laws applicable to the actual service and participants. Screen customers and relevant connected persons, taking account of applicable UN, EU, UK, US or other regimes. Exclude legally barred persons, transactions and territories. Assess potential matches before reaching conclusions. FATF classifications inform the level of scrutiny and required measures rather than proving that every resident is sanctioned. Disclosed provider and risk-based geographic limits can also affect acceptance.

5. Enhanced review

Additional due diligence is used for elevated risks, including complex control structures, PEP connections, adverse findings, geographic exposure and unusual payment behaviour. Political exposure does not itself establish wrongdoing. Seek relevant documents, evidence of funds or wealth, permissions and ownership or wallet explanations. Obtain senior approval where required and review more frequently. A relationship must be rejected or ended if its risk cannot be managed adequately.

6. Ongoing monitoring

Review live activity against the customer's disclosed purpose and expected profile. Appropriate tools include screening, risk rules, blockchain analytics and human investigation. Unusual velocity, suspected theft, ransomware connections, darknet dealings, unexplained third-party funding and evasive structuring warrant examination. Evaluate indirect links and mixer exposure in context. Record the reasoning and obtain supporting commercial evidence where necessary. Monitoring is risk-sensitive and cannot promise perfect detection.

7. Travel Rule and restricted activity

Applicable transfer-information rules determine which sender and recipient details must be obtained, checked, kept and exchanged securely. Missing required data can lead to restriction or rejection, including for self-hosted-wallet transfers where relevant. Criminal proceeds, exploitation, counterfeit goods, shell banking, unlawfully unlicensed financial services and concealed ownership are unacceptable. Processing undisclosed third-party business is prohibited. Regulated or higher-risk sectors need express approval and evidence of lawful operation.

8. Investigations, restrictions and reporting

Escalated matters require documented evaluation by authorised personnel. Seek relevant clarification and apply proportionate account or transaction limits as necessary. Holding, returning or freezing assets requires both actual control and legal authority. Any return must consider ownership, lawful destination and sanctions. Restrictions do not automatically extinguish customer entitlements. Statutory reports go to the competent authority, with appropriate cooperation and confidentiality. Legal anti-tipping-off duties can prevent disclosure of an investigation.

9. Records, training and oversight

Records must allow authorised reconstruction of verification, payments and compliance decisions while preventing unauthorised access or alteration. A five-year baseline follows closure for due diligence and each transaction for transaction records, with applicable law controlling different periods. Preserve longer where lawfully required. Apply the Privacy Policy. Train staff for their roles, review control effectiveness and correct deficiencies. Revisit the Policy annually at minimum and when risk, services or law materially changes.

10. Cooperation and contact

Customers must cooperate with proportionate verification, keep records accurate and use services only for the accepted activity. Material changes require prompt disclosure. Inadequate cooperation can block activation or justify restrictions under the Terms. Each participant retains the duties assigned to it by law even when a provider performs checks. Compliance questions go to info@clirizo.com. Updates are available at clirizo.com and material changes are notified where required.