# Privacy Policy

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

## 1. Scope and data responsibility

Personal information used for the Clirizo website, onboarding and available merchant services is covered here. The operator determines the purposes of processing for which it acts as controller. Other providers and merchants can be independent controllers, with separate privacy responsibilities. Where a party acts solely on instructions, contractual and legal rules define that role. Privacy enquiries belong at info@clirizo.com.

## 2. Information and sources

We process information needed for the relationship, such as names, contact details, business activity, ownership, account security records, IP and device information, messages and complaints. Identity evidence, funding information and blockchain payment records apply where relevant functions require them. Sources include you, business representatives, merchants, service providers, lawful compliance sources and public registers or blockchains. When supplying another person's data, establish a lawful basis and inform them appropriately.

## 3. Purposes and lawful grounds

We use data to assess applications, administer the relationship, deliver enabled functions, respond to enquiries, prevent abuse and meet legal duties. Applicable grounds include steps requested before contracting, contract performance, legal obligations, legitimate interests subject to balancing, and consent. Optional activities requiring consent must permit withdrawal. Accepting service terms is not blanket permission for unrelated uses. Missing mandatory information can prevent service delivery. Personal data is not sold.

## 4. Verification and automated assessments

Financial crime prevention can require identification, beneficial ownership review, sanctions and politically exposed person screening, blockchain analysis and legally mandated originator or beneficiary information. Explain any biometric verification before collection and establish the necessary legal basis. Automated systems can assist risk assessment. Individuals have applicable rights to challenge significant solely automated outcomes and request human intervention, subject to lawful confidentiality limits. Contact info@clirizo.com to raise a concern.

## 5. Sharing and cross-border processing

Disclosure is limited to legitimate needs of infrastructure, communications, support, security, identity and compliance providers, payment participants, advisers and legally entitled authorities. Providers acting for the operator require appropriate contractual protection. Other controllers handle their own obligations. Any lawful transfer of the business must protect relevant data. Cross-border transfers follow the applicable restrictions and authorised mechanisms. Further information or copies of applicable safeguards, subject to lawful redaction, are available through info@clirizo.com.

## 6. Cookies and preferences

The site can use cookies and local storage for authentication, protective measures and user preferences. Blocking necessary storage can affect operation. Before optional tracking is introduced, users must receive information about its purpose, suppliers and lifetime and any required consent choice. Withdrawal must remain accessible. Browser settings allow storage to be cleared. This notice does not itself establish that optional tracking is deployed.

## 7. Retention and deletion

Data is kept only while justified by its purpose or a valid preservation duty. Applicable AML records ordinarily follow a five-year baseline after the relationship ends for identification and due diligence, and after each transaction for its record. Local legal requirements control any different trigger or period. Applications and technical logs follow their own justified needs. Legal holds can extend retention. Records then undergo deletion or anonymisation. Public blockchain entries cannot be rewritten by the operator.

## 8. Rights and requests

Depending on applicable law, individuals can obtain information or copies, correct data, request erasure or restriction, seek portability, object and withdraw consent. Automated-decision rights also apply where provided. Contact info@clirizo.com, with proportionate verification when necessary. Statutory response periods govern, and charges arise only under lawful exceptions. Requests can be limited by required records, confidentiality or the rights of others. Available explanations and appeal routes will be given. A competent supervisory authority can also receive complaints.

## 9. Data Security and Incident Management

Information protection combines appropriate access controls, authentication, secure communications, logging and safeguards for retained data. Incidents require investigation and corrective action, including required notices to authorities or individuals. Absolute security cannot be guaranteed. The service is intended for people aged at least 18. Notify info@clirizo.com about suspected misuse or a child's data. Policy revisions are published on clirizo.com. Material changes are communicated and new consent obtained when the applicable rules require it.