

Privacy Policy

Effective Date: 23 September 2025

Welcome to the ReqWire Privacy Policy (the “Policy”). It explains how we collect, use, share, retain, and delete personal data obtained through <https://reqwire.io> (the “Website” or “Platform”).

“Personal data” means any information relating to an identified or identifiable natural person.

This Policy covers Personal data we collect when you:

1. visit or use the Website, and/or
2. apply for services or complete customer onboarding forms.

It also applies to data you provide for newsletters, events, and other marketing.

Please read this Policy together with our Cookie Policy.

1) Important Information & Who We Are

This Policy explains how ReqWire collects and processes your Personal data.

The Website is owned and operated by **ReqWire Ltd.**, a limited liability company organized under the laws of Saint Vincent and the Grenadines (“ReqWire”, “we”, “us”, “our”). ReqWire Ltd. acts as the data controller. For privacy enquiries, please contact support@reqwire.io (preferred) or by post at the above address.

2) Controllers

ReqWire is the controller responsible for your Personal data for the activities described here. Certain activities may involve **joint controllers** (e.g., identity verification providers, payment or onboarding service providers, and affiliated companies), who may determine purposes and means of processing alongside us.

We provide our services via partners:

Layer2: <https://layer2financial.com/privacy-policy/>

For onboarding/KYC these partners and certain screening providers act as independent controllers of your personal data. For payment execution they may act as our processors.

Their own privacy notices describe their processing in more detail. Review any third-party terms before using integrated features. We aim to **minimize** Personal data we store directly whenever feasible.

3) Changes to this Policy & Your Duty to Inform Us

We may update this Policy from time to time.

Keep your Personal data **accurate and current**. Please notify us of changes during your relationship with us.

4) Third-Party Links

Our Website may include links to third-party sites, plug-ins, and applications. Clicking those may allow third parties to collect or share data about you. We do not control those sites. Review their privacy notices before use.

5) GDPR

For EU/EEA users, we process Personal data in accordance with the **General Data Protection Regulation (EU) 2016/679 (GDPR)**.

6) Glossary (Key Terms)

- **Data Subject:** a living individual about whom we process Personal data.
- **Controller:** the party determining why/how Personal data is processed.
- **Processor:** the party processing Personal data on behalf of a controller.
- **Personal Data:** information identifying a person directly or indirectly (e.g., name, address, ID, email, IP, device identifiers).
- **Processing:** any operation performed on Personal data (collect, use, store, share, delete, etc.).
- **Special Categories:** sensitive data (e.g., health, ethnicity, religion, union membership). Processed only under strict conditions.

Note: data relating to legal persons (e.g., company name, registration number) is **not** Personal data, though we treat it confidentially.

7) Data We Collect

We may collect, use, store, share, and disclose the following categories (illustrative list):

- **Identity Data:** name, surname/maiden name (if applicable), date of birth, nationality, gender, ID/passport numbers, user IDs.
- **Contact Data:** residential/billing address, email, phone.
- **Technical & Usage Data:** IP address, device IDs, browser type/version, time zone, OS, pages viewed, clicks, response times, errors, session duration, navigation paths.
- **Website Visit Data:** URLs, clickstream, interaction data (scrolls, clicks, mouse-overs).
- **Marketing & Communications Data:** subscriptions, preferences, event participation.
- **Transaction/Service Data:** information necessary to provide requested services (e.g., onboarding answers, funding, transfers), wallet addresses, blockchain transaction hashes, public keys, counterparties/payees/beneficiaries, IBANs/account numbers, payment references, exchange or conversion details, fraud-risk and sanctions/PEP screening results, and any data you voluntarily provide.

We also create **Aggregated Data** (statistics/demographics) that does not identify you. If aggregated data can identify you when combined, we treat it as Personal data.

Age: Services are not intended for children under 18. If collected inadvertently, we will delete it promptly.

8) If You Fail to Provide Data

If we need data by **law** or for **legitimate interests** (e.g., identity checks, risk mitigation, onboarding decisions) and you don't provide it (or provide insufficient data), we may be unable to offer services or conclude an agreement.

9) Special Categories

We do **not** knowingly collect Special Category data. If a purpose requires it, we will request explicit consent or rely on a GDPR legal basis where applicable.

10) How We Collect Data

- **Direct interactions:** forms, email, phone, support chats, event sign-ups, newsletter sign-ups.
- **Automated means:** cookies, logs, and similar technologies (see Cookie Policy).
- **Third parties/public sources:** analytics providers, ad networks, search engines; KYC/AML providers performing identity and sanctions checks; payment and onboarding partners.

Automated decision-making & profiling (Art. 22 GDPR): We use automated systems to assess onboarding risk and eligibility, including identity, sanctions and fraud-risk scoring. These decisions may produce legal or similarly significant effects (e.g., account approval or denial). You have the right to obtain human review, to express your view, and to contest such decisions.

11) Legal Bases for Processing

We process your Personal data only where lawful, including:

- **Contract:** to perform (or take steps to enter into) a contract with you.
- **Legitimate Interests:** to operate and improve our Platform, prevent fraud, protect our business/reputation, and grow responsibly—balanced against your rights.
- **Legal/Regulatory Obligation:** to comply with laws (e.g., AML/CFT, tax, accounting, sanctions screening).
- **Consent:** e.g., certain marketing. You can withdraw consent at any time.

12) Purposes & Legal Bases (Summary)

- **Onboarding & KYC/AML** (Identity, Contact, KYC/AML, Transaction): Contract; Legitimate Interests; Legal Obligation.
- **Service Delivery** (account setup, transfers, invoicing, conversions, statements): Contract; Legal Obligation.
- **Risk/Fraud/Security** (screening, monitoring, incident response): Legitimate Interests; Legal Obligation.
- **Billing & Collections** (invoices, debt recovery): Contract; Legal Obligation; Legitimate Interests.
- **Support & Relationship Management** (notices, updates, queries): Contract; Legitimate Interests.
- **Website Administration** (IT, security, troubleshooting, analytics): Legitimate Interests; Legal Obligation.

- **Marketing & Insights** (newsletters, product updates, measuring effectiveness): Consent (where required); Legitimate Interests.
- **Legal Claims/Compliance**: Legal Obligation; Legitimate Interests.

For details on a specific activity's legal basis, contact support@reqwire.io.

13) Marketing Choices

- We may send marketing where permitted by law (e.g., existing customer soft opt-in) or with your **consent**.
- **Third-party marketing**: we'll obtain your **opt-in** before sharing data with third parties for their marketing.
- **Opt-out** anytime via unsubscribe links or by emailing support@reqwire.io.
- **Cookies**: We participate in an affiliate-marketing program that uses cookies or pixels for referral attribution. Non-essential cookies are set only with your consent. See our Cookie Policy for purposes, retention periods, and instructions to withdraw consent. You can manage cookies in your browser. Some features may not function without certain cookies.

14) Change of Purpose

We will use your data only for the purposes collected unless a compatible purpose arises or we are legally required to process it otherwise. For incompatible uses, we'll notify you and explain the legal basis.

15) Disclosures of Your Personal Data

We may share Personal data with:

- **Service providers**: hosting/infrastructure, KYC/AML, payments, card issuers, CRM, analytics, email delivery.
- **Affiliates/partners**: to help provide services, detect fraud, and inform product decisions.
- **Professional advisers**: auditors, banks, insurers, consultants.
- **Law enforcement/regulators**: where required.
- **Fraud prevention/credit risk organizations**.
- **Debt recovery agencies**.

- **Successors:** in mergers, acquisitions, or asset sales.

We require recipients to process data lawfully, securely, and only for specified purposes under our instructions where acting as processors. Our service providers currently store data in the **EU/EEA (e.g., Germany)**. We'll update this Policy if storage locations change.

16) International Transfers

If we transfer Personal data outside the EEA/UK, we ensure appropriate safeguards, such as:

- **Adequacy decisions**, or
- **EU Standard Contractual Clauses (SCCs)**.

For details, contact support@reqwire.io.

17) Data Security

We use appropriate technical and organizational measures to protect confidentiality, integrity, and availability of Personal data. Access is limited to personnel and processors with a **need-to-know** and subject to confidentiality. We will notify you and/or regulators of data breaches where legally required.

18) Data Retention

We retain Personal data only as long as necessary for the purposes collected and thereafter:

- to comply with **legal, accounting, tax, AML/CFT** obligations; and/or
- to establish, exercise, or defend legal claims.

Typical retention: up to **6 years** after the customer relationship ends (longer where required, e.g., **up to 10 years** for certain accounting/tax records). You may request deletion where applicable (see Rights below).

When processing data revealing criminal-offence information or politically exposed person (PEP) status, we rely on our legal obligations under AML/CTF laws. We apply strict access controls and retain such data only as required by law.

19) Data Minimization

Where feasible, we **anonymize** or **pseudonymize** data once identification is no longer necessary. Anonymized data may be used indefinitely for analytics and research.

20) Your Rights (GDPR)

Subject to conditions and applicable law, you may:

- **Access** your Personal data;
- **Rectify** inaccurate or incomplete data;
- **Erase** data (right to be forgotten);
- **Object** to processing (including direct marketing);
- **Restrict** processing;
- **Port** data (receive it in a structured, commonly used, machine-readable format);
- **Withdraw consent** (where processing is based on consent).

How to exercise: email support@reqwire.io.

- **Fees:** ordinarily none. We may charge a reasonable fee or refuse requests that are manifestly unfounded, excessive, or repetitive.
- **Verification:** we may request information to confirm identity and secure your data.
- **Timing:** we aim to respond within **1 month** (extendable for complex/multiple requests).

21) Complaints

You have the right to complain to your local data protection authority. We'd appreciate the chance to resolve your concerns first—please contact support@reqwire.io.

You may also contact our EU Representative or lodge a complaint with the supervisory authority of the Member State of your habitual residence

22) Contact & Conclusion

We may amend this Policy and will post updates on **reqwire.io**.

Questions, comments, or requests: **support@reqwire.io**.