

Privacy policy

Version 1.0

Reading copy. The authoritative text is the plain-text file whose fingerprint appears below; it is downloadable at the same address with the .txt extension.

SHA-256 fingerprint of the authoritative text : 20e61aeb61765a606ced70071bbb8bf3df5ff4218e7331d496d72596b14df07e

1. Controller and data protection contact

COWRIEX, a Societe par Actions Simplifiee (SAS) with its registered office at Ilot 1678, Quartier Seme, Parcelle q, Maison YVES AOULOU, Abomey-Calavi, Benin, operates the CowriePay platform and determines the purposes and means of the processing described below. Full identification details appear in the Legal notice (www.cowriepay.io/legal/legal-notice).

Data protection contact point: privacy@cowriepay.io. Write to that address with any question, or to exercise your rights.

2. Who is concerned

CowriePay is a service for businesses. The people whose data we process are therefore not all our customers:

- visitors to the www.cowriepay.io website;
- people who write to us, through the contact form or the chat window;
- people authorised by a business customer to use the dashboard or the API;
- people whose identity must be verified when a business customer is onboarded: directors, ultimate beneficial owners, signatories;
- people appearing in transaction data, in particular through the blockchain address a payment is received from.

Where our customer uses CowriePay to serve its own customers, the allocation of roles is set out in article 12.

3. Data we collect

A. Website visitors

- Traffic statistics produced by our own audience-measurement tool, which stores nothing in your browser: pages viewed, referring page, device and browser type, language and approximate country. A technical visit identifier, renewed every day, is computed on our servers from your IP address and your browser; the IP address itself is not retained.
- Your language choice, if you express one, kept in your browser.
- On the contact page, an anti-bot check provided by a third party.

B. People who contact us

- Contact form: name, email address, company name and the content of your message.
- Chat window: the content of the exchange and, if you provide them, your contact details. The chat loads only if you open it.

C. Dashboard and API users

- Identity and account: name, email address, language, role within the workspace.
- Security: password (kept as a cryptographic hash, itself encrypted, never in clear text), one-time authentication

factor, session tokens, IP addresses allowed for an API key.

- Logging: timestamps of sign-ins and sensitive actions, with the associated IP address.

D. People verified at onboarding

- Business: name, country and registration number, website, activity, expected monthly volume.
- Individuals: first and last names, date of birth, nationality, country of residence, address, identity-document type and number, issuing country and expiry date, ownership percentage, email address, telephone, national identification reference where one exists, and politically-exposed-person status as declared by the person themselves.
- Supporting documents: certificate of incorporation, identity document, proof of address, bank statement.

We collect and process no biometric data: no verification photograph, no liveness detection, no facial comparison.

E. Mandatory and optional information

The first and last names of a director or beneficial owner, and their capacity, are required as soon as they are recorded. Their date of birth, nationality, country of residence, address, the type, number and issuing country of their identity document, and the ownership percentage for a beneficial owner, condition access to production: for as long as they are missing, that access is refused. A signatory falls under a lighter information tier.

Business information and supporting documents may be provided progressively, but an incomplete or inaccurate file cannot be approved, and obliges us to end the relationship if it remains so.

The information you send us through the contact form or the chat window is optional: its absence only prevents us from answering you usefully.

F. Origin of data you did not give us

- Where you are a director, beneficial owner or signatory of a business customer, your data most often reaches us from that company, which warrants to us that it is entitled to pass it on and to inform you of this.
- Blockchain addresses and transaction characteristics are read from public, permanent registers that we do not feed.
- Screening results come from the list of designated addresses published by the Office of Foreign Assets Control.

G. Transaction data

- Blockchain addresses, including the origin address of a deposit, amounts, assets, networks, transaction identifiers and timestamps.
- Address-screening results.
- References the customer chooses to attach to a wallet or to one of its own customers. These references must be opaque identifiers: the customer undertakes to place no personal data in clear text there.

4. Purposes and legal bases

Benin law recognises as legal bases consent, performance of a contract or of pre-contractual measures, compliance with a legal obligation, protection of vital interests, and performance of a public-interest task. Our processing rests on the first three:

Purpose | Legal basis

Providing the service: account creation, authentication, wallet creation, deposit detection, execution of payouts, reporting of transactions | Performance of the contract

Securing the service: strong authentication, withdrawal controls, protection against unauthorised access and abuse, logging | Performance of the contract and legal obligation

Verifying the business customer and identifying its beneficial owners, screening addresses, retaining records and producing the required reports | Legal obligation

Answering your requests and providing support | Performance of the contract or pre-contractual measures

Measuring website traffic and detecting abnormal usage | Performance of the contract, for the provision and security of the site; no data is used for advertising or passed to a third party

Sending you commercial communications | Consent, withdrawable at any time

5. Automated processing

Screening of blockchain addresses is automated. Its logic is as follows: the address concerned is compared, character by character, with the addresses on the list of designated addresses published by the Office of Foreign Assets Control. It is an exact match. No score, no probability, no behavioural profile and no data about you other than the address itself enters that comparison.

A match, or the impossibility of running that comparison, automatically results in the transaction being held: a deposit is not credited, a payout is not sent.

An automatic hold can only be lifted by human review: our authorised staff decide whether to release the transaction or maintain the measure. You may ask us to reconsider a decision by writing to privacy@cowriepay.io. Where the law prohibits us from disclosing the reason for a measure, we comply with that prohibition.

We carry out no commercial profiling and no automated scoring of individuals.

6. Recipients and processors

We sell no data. We share what is strictly necessary with:

Provider | Role | Location

Contabo GmbH | Hosting of production systems | Germany

Cloudflare, Inc. | Storage of verification documents and anti-bot checks on forms | United States and global network

Mailjet | Delivery of transactional emails | European Union

GetBlock | Access to blockchain networks (reading and broadcasting transactions) | Outside Benin

Our audience measurement and our support tool run on our own servers: the corresponding data is passed to no third party.

We also disclose data to the competent authorities where the law requires it, and to our professional advisers bound by confidentiality.

Finally, the transactions you carry out are recorded on public blockchains. Those records are visible to anyone, permanent and outside our control: we can neither amend nor delete them.

7. Transfers outside Benin

Our production systems are hosted in the European Union, in Munich, Germany, by Contabo GmbH. Some of the providers listed in article 6 process data from other countries.

These transfers are limited to what is necessary to provide the service and are framed by contractual confidentiality and security commitments with each provider. Benin law subjects transfers to a third country to formalities with the Personal Data Protection Authority; we are carrying out the corresponding steps.

8. Retention periods

The periods below are the ones our systems actually apply. Several of them follow from anti-money-laundering record-keeping obligations and are technically locked: the records concerned cannot be deleted, including by us.

Category | Period

Financial records: deposits, payouts, internal transfers, refunds | 10 years. Deletion is refused by the database

itself.

Audit log of sensitive actions, including the author's IP address | 10 years. The register is append-only: entries can be read but can be neither amended nor deleted.

Verification file and supporting documents | Duration of the relationship, then 10 years under record-keeping obligations.

Screening results | At least 10 years. These records are not subject to an automatic purge.

Notification delivery logs, including the content of the event sent to the customer | 90 days.

Outbound email queue, the content of which is encrypted | 30 days.

Unaccepted invitations | Neutralised 30 days after they expire.

Session tokens | One hour at most for the access token, 7 days for the refresh token.

Messages received through the contact form | As long as needed to handle your request and follow up the commercial relationship.

9. Your rights

You have rights of access, rectification, erasure, restriction, objection and portability, as well as the right to withdraw your consent at any time where processing rests on it. Withdrawing is as easy as consenting.

To exercise these rights, write to privacy@cowriepay.io. We may ask for material allowing us to verify your identity. We respond within thirty days.

The limits, stated plainly

- Legal record-keeping obligations override the right to erasure: until the applicable period has elapsed, we cannot delete a financial record or a verification file.
- The audit log is an append-only register, and the database refuses any modification or deletion. It contains IP addresses among other things. An erasure request therefore cannot be satisfied on that register before its retention period expires.
- Records on public blockchains are irreversible and outside our control.
- Where we cannot grant a request, we explain why, except where the law prohibits us from doing so.

If you consider that your rights are not being respected, you may refer the matter to the Personal Data Protection Authority (APDP) of Benin, as well as to the competent courts.

10. Security

We apply technical and organisational measures proportionate to the sensitivity of a custody service:

- encryption of the most sensitive items through a dedicated key-management service: password hashes, API secrets, notification signing secrets, payout destination addresses, email content and contact details;
- separation of the signing system: the keys allowing assets to be moved are isolated in a distinct component that the main application cannot access;
- two-factor authentication, mandatory for sensitive operations initiated from the dashboard;
- outbound controls: destination allowlist, a cooling-off period on any new destination, per-transaction and rolling 24-hour caps, and second-person approval where that option is enabled;
- restricted access to verification documents, available only through time-limited links;
- append-only logging of sensitive actions, with the database refusing any modification or deletion.

No system is immune to an incident. The security of your account also depends on protecting your credentials, your API keys and your authentication factors.

11. Data breaches

In the event of a data breach likely to create a risk for the people concerned, we make the required notifications to the competent authority and inform the people concerned as soon as possible.

Notice is given by email and, for dashboard users, displayed in the dashboard. We state the nature of the incident, the categories of data concerned, the likely consequences and the measures taken or recommended.

12. Data of our customers' own customers

The service is designed so that we receive as little data as possible about our customers' own customers. The allocation of roles follows from that.

- We are the controller for everything that falls under our own obligations: verification of the business customer, identification of its directors and beneficial owners, address screening, logging and retention of records. In that scope we do not act on instructions and the business customer cannot relieve us of them.
- We do not, in principle, receive end customers' personal data. The references a business customer attaches to a wallet or to one of its customers must be opaque identifiers, and the Terms and conditions (www.cowriepay.io/legal/terms) require this of it.
- If a business customer nevertheless sends us end customers' personal data in those free-text fields, we process it solely to provide the service and only on that customer's instructions: we then act as its processor, it remains the controller, and it is for it to inform its customers and to hold a legal basis.

We make no commercial use of the data a business customer entrusts to us and use it for no purpose other than providing the service.

A business customer needing a formal data processing agreement, separate from this policy, may request one at privacy@cowriepay.io.

13. Minors

CowriePay is a service for businesses and is not intended for minors. We do not knowingly collect data relating to minors. Were such collection to come to our attention, we would delete the data concerned, subject to record-keeping obligations.

14. Changes

We may amend this policy to reflect changes in the service or in the applicable framework. The date of last update appears at the top of the page. In the event of a substantial change we inform dashboard users by email or in the dashboard.

In the event of any discrepancy between language versions, the French version prevails.