PRIVACY POLICY

Effective Date: March 16, 2026

Last Updated Date: March 16, 2026

PLEASE READ THIS PRIVACY POLICY CAREFULLY. IT DESCRIBES HOW COREACCESS SOLUTIONS S.A. COLLECTS, USES, STORES, SHARES, AND PROTECTS YOUR PERSONAL DATA IN CONNECTION WITH YOUR ACCESS TO AND USE OF OUR SERVICES. BY ACCESSING OR USING THE SERVICES, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD THIS PRIVACY POLICY.

1. Introduction

COREACCESS SOLUTIONS S.A. ("COREACCESS", "we", "us", or "our") is a company incorporated under the laws of the Republic of Panama, with registration number 155771915 and registered address at World Trade Center, 7th Floor, 53E Street, Marbella, Bella Vista, Panama City, Republic of Panama.

We operate a digital platform and provide access to a range of digital asset-related services, software, infrastructure, and technology services, including onboarding, account-related, wallet-related, transaction-related, API, dashboard, administrative, informational, support, and related digital services (collectively, the "Services"). Certain Services may be provided directly by COREACCESS or through third-party providers, vendors, blockchain networks, wallets, payment rails, compliance vendors, custodians, infrastructure partners, or similar service providers. The Services are accessible through our website at coreaccess.solutions (the “Website") and any associated applications, interfaces, or platforms (collectively, the "Platform").

This Privacy Policy ("Policy") explains how we collect, use, store, disclose, and otherwise process personal data about individuals who access or use the Services, visit the Platform, or otherwise interact with us. It also describes your rights in relation to your personal data and how you may exercise them.

This Policy should be read together with our Terms of Use and any other notices or policies we may publish from time to time in connection with specific Services or processing activities. In the event of any conflict between this Policy and a more specific notice, the more specific notice shall prevail to the extent of the conflict.

If you do not agree with this Policy, please do not access or use the Services.

2. Scope of this Privacy Policy

This Policy applies to:

- individuals who register for or use the Services ("Users");
- visitors to the Platform or any associated website or application;
- individuals who contact us for support, information, or other purposes;

- individuals whose personal data we receive in connection with the provision of the Services, including in the context of onboarding, compliance, or transaction processing; and
- any other individuals whose personal data we process in connection with our business operations.

This Policy does not apply to the data practices of third-party providers, partners, or services that may be accessible through or in connection with the Platform. Such third parties operate under their own privacy notices and data protection practices, for which COREACCESS is not responsible. We encourage you to review the privacy notices of any third-party services you access.

The categories of personal data we collect, the purposes for which we process it, and the rights available to you may vary depending on the nature of the Services you use, your jurisdiction of residence, and applicable legal and regulatory requirements.

3. Who We Are / Data Controller Information

For the purposes of this Policy, COREACCESS SOLUTIONS S.A. acts as the data controller (or equivalent responsible entity under applicable law) in respect of personal data processed in connection with the Services.

Our details are as follows:

Company name: COREACCESS SOLUTIONS S.A.

Registration number: 155771915

Registered address: World Trade Center, 7th Floor, 53E Street, Marbella, Bella Vista, Panama City, Republic of Panama

Privacy contact: contact@coreaccess.solutions.

Where we engage third-party service providers to process personal data on our behalf, such providers act as data processors (or equivalent) and are required to process personal data only in accordance with our instructions and applicable law.

4. Categories of Personal Data We Collect

Depending on the Services you use, your jurisdiction, and applicable legal and regulatory requirements, we may collect and process the following categories of personal data:

4.1 Identification and Contact Data

- Full legal name, date of birth, nationality, and country of residence;
- Government-issued identification documents (e.g., passport, national identity card, driver's licence, or equivalent);
- Residential address and proof of address documentation;
- Email address, telephone number, and other contact details;
- Tax identification numbers, social security numbers, or equivalent identifiers, where required by applicable law.

4.2 Account and Profile Information

- Username, account credentials, and authentication information;
- Account settings, preferences, and profile information;
- Records of account activity, login history, and session data;
- Communications and correspondence with us, including support requests and inquiries.

4.3 Onboarding, Verification, and KYC / KYB Information

- Identity verification documentation and data, including images of identification documents and liveness or biometric verification data where applicable;
- Source of funds and source of wealth information and supporting documentation;
- Business registration documents, corporate structure information, and beneficial ownership information, where applicable;
- Risk assessment and due diligence information;
- Information obtained from sanctions lists, politically exposed persons ("PEP") databases, adverse media sources, and other compliance screening tools;
- Information obtained from blockchain analytics providers, transaction monitoring tools, and fraud-prevention services.

4.4 Transaction-Related Information

- Details of transactions initiated, processed, or facilitated through the Services, including amounts, currencies, digital asset types, timestamps, and counterparty information;
- Wallet addresses, transaction hashes, and blockchain-related identifiers;
- Payment-related information, including bank account details, payment instrument details, and related financial information, where applicable;
- Records of instructions submitted through the Platform.

4.5 Device, Technical, and Usage Information

- IP address, device identifiers, browser type and version, and operating system;
- General geographic location derived from IP address or device settings;
- Log data, access records, and usage data relating to your interactions with the Platform;
- Cookies and similar tracking technology data, as further described in Section 9.

4.6 Communications Data

- Content of communications you send to us, including emails, support tickets, and chat messages;
- Records of marketing communications sent to you and your preferences;
- Feedback, survey responses, and other information you voluntarily provide.

4.7 Information from Third Parties and Public Sources

- Information received from identity verification providers, KYC/AML service providers, credit reference agencies, and sanctions screening providers;
- Information obtained from public registries, regulatory databases, and publicly available sources;

- Information received from business partners, referral sources, or other third parties in connection with the Services;
- Information obtained from blockchain analytics providers or transaction monitoring services.

We may also collect any other information you voluntarily provide to us in connection with your use of the Services or your interactions with us. Where we are required to collect certain personal data by law or under the terms of our agreement with you, and you fail to provide that data, we may be unable to provide the Services or may be required to restrict or suspend your access.

5. How We Collect Personal Data

We collect personal data through the following means:

5.1 Directly from You

We collect personal data directly from you when you: register for an account or apply to use the Services; complete onboarding or verification processes; submit transactions or instructions through the Platform; contact us for support or with inquiries; respond to surveys or communications; or otherwise interact with us or the Platform.

5.2 Automatically

We automatically collect certain technical and usage data when you access or use the Platform, including through the use of cookies, web beacons, log files, and similar technologies. This includes information about your device, browser, IP address, and interactions with the Platform. Please refer to Section 9 for further information on our use of cookies and similar technologies.

5.3 From Third Parties

We may receive personal data about you from third parties, including: identity verification and KYC/AML service providers; sanctions screening and fraud-prevention providers; blockchain analytics providers; business partners and referral sources; publicly available sources and databases; and other third parties in connection with the provision of the Services or our compliance obligations.

6. Purposes of Processing

We process personal data for the following purposes, subject to applicable law:

- Providing, operating, maintaining, and improving the Services and the Platform;
- Account creation, administration, and management;
- Onboarding, user verification, and customer support;
- Identity verification, KYC, KYB, AML, sanctions screening, fraud prevention, transaction monitoring, and other compliance and risk management activities;
- Processing and facilitating transactions and instructions submitted through the Platform;
- Communicating with you regarding the Services, your account, transactions, security alerts, and administrative matters;

- Sending marketing and promotional communications where permitted by applicable law and in accordance with your preferences;
- Conducting analytics, monitoring platform performance, and improving user experience;
- Complying with applicable legal, regulatory, tax, accounting, and reporting obligations;
- Enforcing our Terms of Use and other legal agreements;
- Protecting the rights, property, and safety of COREACCESS, our users, and third parties;
- Detecting, investigating, and preventing fraud, unauthorized access, security incidents, and other unlawful or prohibited activities;
- Responding to requests, complaints, and inquiries from users and third parties;
- Conducting internal business operations, including audits, risk assessments, and business planning;
- Exercising or defending legal claims and rights;
- Any other purpose described to you at the time of collection or for which you have provided your consent.

7. Legal Bases for Processing

Where applicable law requires us to identify a legal basis for processing personal data, we rely on one or more of the following:

7.1 Performance of a Contract

Processing is necessary to perform our obligations under our Terms of Use or any other agreement with you, or to take steps at your request prior to entering into such an agreement. This includes processing necessary to provide the Services, manage your account, and process transactions.

7.2 Compliance with Legal Obligations

Processing is necessary to comply with applicable legal and regulatory obligations, including obligations relating to anti-money laundering, counter-terrorism financing, sanctions compliance, tax reporting, record-keeping, and other regulatory requirements applicable to our business.

7.3 Legitimate Interests

Processing is necessary for the purposes of our legitimate interests or those of third parties, where such interests are not overridden by your interests or fundamental rights and freedoms. Our legitimate interests include: operating and improving the Services; maintaining the security and integrity of the Platform; preventing fraud and financial crime; enforcing our legal terms; and conducting internal business operations.

7.4 Consent

Where we rely on your consent as the legal basis for processing, we will obtain your consent prior to processing. You may withdraw your consent at any time by contacting us using the details in Section 18. Please note that withdrawal of consent does not affect the lawfulness of processing carried out prior to withdrawal, and may affect our ability to continue providing certain Services.

The legal bases described above are presented for informational purposes and reflect internationally recognised data protection principles. The specific legal basis applicable to any given processing activity will depend on the nature of the Services, your jurisdiction, and applicable law.

8. KYC, AML, Sanctions, and Compliance-Related Processing

As part of our commitment to operating a compliant and responsible platform, and in order to meet our legal and regulatory obligations, we conduct a range of compliance-related processing activities. These activities may include, without limitation:

- Know-Your-Customer ("KYC") and Know-Your-Business ("KYB") verification, including identity verification, document checks, and due diligence procedures;
- Anti-money laundering ("AML") screening and monitoring, including transaction monitoring and suspicious activity assessment;
- Sanctions screening against applicable sanctions lists and databases maintained by relevant authorities;
- Politically exposed persons ("PEP") screening and enhanced due diligence where required;
- Source-of-funds and source-of-wealth assessments;
- Blockchain analytics and on-chain transaction analysis, including the use of third-party blockchain analytics tools;
- Adverse media and reputational screening;
- Fraud prevention and risk assessment activities;
- Ongoing monitoring of accounts, transactions, and user activity for compliance purposes.

In connection with these activities, we may request additional documents, information, or explanations from you at any time. We may also obtain information from third-party compliance service providers, public databases, sanctions lists, and other external sources.

Where required or permitted by applicable law, we may disclose personal data to regulators, law enforcement agencies, financial intelligence units, supervisory authorities, banks, compliance vendors, counterparties, auditors, and professional advisers. Such disclosures may be made without prior notice to you where required or permitted by law.

Failure to provide information requested in connection with our compliance obligations may result in us being unable to provide the Services, or in the suspension, restriction, or termination of your access to the Services.

9. Cookies and Similar Technologies

We and our third-party service providers may use cookies, web beacons, pixel tags, local storage, and similar tracking technologies (collectively, "Cookies") when you access or use the Platform. Cookies are small data files placed on your device that allow us to recognise your browser or device and collect certain information about your interactions with the Platform.

We may use Cookies for the following purposes:

- Essential / functional Cookies: to enable core Platform functionality, authentication, and security features;
- Analytics and performance Cookies: to understand how users interact with the Platform, measure performance, and improve user experience;
- Security Cookies: to detect and prevent fraud, unauthorized access, and other security risks;
- Preference Cookies: to remember your settings and preferences;
- Marketing and advertising Cookies: where applicable and permitted by law, to deliver relevant content and measure the effectiveness of communications.

You may be able to manage or disable certain Cookies through your browser settings or through any cookie preference tool we make available on the Platform. Please note that disabling certain Cookies may affect the functionality of the Platform or your ability to access certain features of the Services.

For more detailed information about our use of Cookies and your options, please refer to our Cookie Policy, available at [Cookie Policy Link], or contact us using the details in Section 18.

Our Platform does not currently respond to browser-level "Do Not Track" signals. We will honour applicable global privacy signals to the extent required by law.

10. How We Share Personal Data

We do not sell your personal data to third parties. We may share your personal data with the following categories of recipients, to the extent necessary and in accordance with applicable law:

10.1 Affiliates and Group Companies

We may share personal data with our affiliates, subsidiaries, and group companies for internal business, operational, compliance, and administrative purposes.

10.2 Service Providers and Data Processors

We engage third-party service providers to perform functions on our behalf, including: identity verification and KYC/AML providers; sanctions screening and fraud-prevention providers; blockchain analytics providers; cloud hosting, IT infrastructure, and data storage providers; analytics, CRM, and communications platforms; customer support providers; payment, banking, wallet, custody, liquidity, and infrastructure partners; and other vendors and processors engaged in connection with the Services. Such providers are required to process personal data only in accordance with our instructions and applicable law.

10.3 Compliance, Regulatory, and Law Enforcement Authorities

We may disclose personal data to regulators, supervisory authorities, financial intelligence units, tax authorities, law enforcement agencies, courts, and other competent authorities where required or permitted by applicable law, including in connection with our AML, sanctions, and other compliance obligations. Such disclosures may be made without prior notice to you where required or permitted by law.

10.4 Professional Advisers and Auditors

We may share personal data with our legal advisers, auditors, accountants, insurers, and other professional advisers where necessary for the purposes of obtaining professional advice, conducting audits, or managing legal claims.

10.5 Transaction Counterparties and Infrastructure Partners

In connection with the processing of transactions or the provision of certain Services, we may share relevant personal data with counterparties, transaction participants, blockchain networks, wallet providers, payment rails, and other infrastructure partners as necessary to facilitate the relevant transaction or service.

10.6 Business Transfers

In the event of a merger, acquisition, sale of assets, reorganisation, financing, change of control, or similar transaction, or in the event of insolvency or bankruptcy proceedings, personal data may be transferred to the relevant counterparty or successor entity as part of that transaction, subject to applicable law.

10.7 With Your Consent

We may share personal data with other third parties where you have provided your express consent to such sharing.

We may also share aggregated, anonymised, or de-identified information that cannot reasonably be used to identify you, for analytical, research, or business purposes.

11. International Data Transfers

COREACCESS operates internationally, and your personal data may be transferred to, stored in, accessed from, or processed in countries other than your country of residence, including countries that may not provide the same level of data protection as your home jurisdiction.

Such transfers may occur in connection with the provision of the Services, the engagement of third-party service providers, compliance activities, or our internal business operations. Recipients of personal data in other jurisdictions may include service providers, affiliates, regulators, and other parties described in Section 10.

Where personal data is transferred internationally, we take reasonable steps to ensure that it is protected in a manner consistent with this Policy and applicable law. Such steps may include contractual protections, data processing agreements, or other mechanisms recognised under applicable law. By providing us with your personal data and using the Services, you acknowledge that your personal data may be transferred to and processed in jurisdictions outside your country of residence.

If you have questions about international data transfers or the safeguards we apply, please contact us using the details in Section 18.

12. Data Retention

We retain personal data for as long as necessary to fulfil the purposes for which it was collected, including to provide the Services, maintain your account, comply with our legal and

regulatory obligations, resolve disputes, enforce our agreements, and protect our legitimate interests.

Retention periods vary depending on the nature of the personal data, the purposes for which it is processed, and applicable legal and regulatory requirements. In particular:

- Personal data collected in connection with KYC, AML, and compliance obligations may be retained for the minimum periods required by applicable law, which may extend beyond the termination of your account or your use of the Services;
- Transaction records and related documentation may be retained for periods required by applicable tax, accounting, regulatory, or record-keeping obligations;
- Personal data processed in connection with legal claims or disputes may be retained for the duration of the relevant proceedings and any applicable limitation periods;
- Personal data processed for fraud prevention and security purposes may be retained for periods necessary to protect against future risks.

Where we are no longer required to retain personal data, we will delete or de-identify it in accordance with our internal data management procedures. Where technical or operational constraints prevent immediate deletion, we will implement reasonable measures to restrict further processing of that data pending deletion.

13. Data Security

We maintain a range of technical, organisational, and administrative security measures designed to protect personal data against unauthorised access, use, disclosure, alteration, loss, or destruction. These measures are designed to be appropriate to the nature of the personal data we process and the risks associated with our processing activities.

Notwithstanding the foregoing, no security measures are infallible or guaranteed to be completely effective. We cannot warrant or guarantee the absolute security of any personal data. In the event of a security incident that affects personal data under our control, we will investigate the matter and, where required by applicable law, notify affected individuals and relevant authorities, and take other remedial steps in accordance with our legal obligations.

You are responsible for maintaining the security of your account credentials and for any activity that occurs under your account. You should notify us immediately if you become aware of any unauthorised access to or use of your account.

14. Your Rights

Depending on your jurisdiction of residence and applicable law, you may have certain rights in relation to your personal data. These may include:

- Right of access: the right to request confirmation of whether we hold personal data about you and, where applicable, to receive a copy of that data;
- Right to rectification: the right to request that we correct or update personal data that is inaccurate or incomplete;
- Right to erasure: the right to request the deletion of your personal data in certain circumstances, subject to our legal and regulatory obligations to retain certain records;

- Right to restriction of processing: the right to request that we restrict the processing of your personal data in certain circumstances;
- Right to data portability: the right to receive your personal data in a structured, commonly used, and machine-readable format, where applicable;
- Right to object: the right to object to the processing of your personal data in certain circumstances, including processing based on legitimate interests;
- Right to withdraw consent: where processing is based on your consent, the right to withdraw that consent at any time, without affecting the lawfulness of processing carried out prior to withdrawal;
- Right to non-discrimination: we will not discriminate against you for exercising any privacy rights available to you under applicable law.

Please note that these rights are not absolute and may be subject to limitations and exceptions under applicable law. In particular, we may be required to retain certain personal data to comply with our legal and regulatory obligations, including AML, KYC, and record-keeping requirements, and we may be unable to delete or restrict processing of such data upon request.

To exercise any of your rights, please contact us using the details provided in Section 18. We will take reasonable steps to verify your identity before responding to any request. We will endeavour to respond to requests within a reasonable timeframe and in accordance with applicable law. We reserve the right to charge a reasonable fee or decline requests that are manifestly unfounded, excessive, or repetitive.

If you are not satisfied with our response, you may have the right to lodge a complaint with the applicable data protection or privacy authority in your jurisdiction, as further described in Section 19.

15. Third-Party Websites and Services

The Platform may contain links to, or integrate with, third-party websites, applications, or services that are not owned or operated by COREACCESS. This Policy does not apply to such third-party services, and we are not responsible for the privacy practices, data handling, or security measures of any third party.

Certain Services may be provided through or in connection with third-party providers, including blockchain networks, wallet providers, payment rails, compliance vendors, custodians, and infrastructure partners. Such third-party services may be subject to separate terms and privacy notices, which we encourage you to review.

We do not control the privacy or security practices of third parties, nor the jurisdictions in which they process data. Any interaction you have with a third-party service is at your own risk, and we accept no responsibility or liability for the data practices of any third party.

16. Children's Privacy

The Services are not directed to, and are not intended for use by, individuals under the age of eighteen (18) years, or such other minimum age as may be required by applicable law in the relevant jurisdiction. We do not knowingly collect personal data from minors.

If we become aware that we have inadvertently collected personal data from a person under the applicable minimum age, we will take prompt steps to delete that information from our records. If you believe that we may hold personal data about a minor, please contact us immediately using the details provided in Section 18.

17. Changes to this Privacy Policy

We may update or amend this Policy from time to time to reflect changes in our data processing practices, the Services, applicable law, or for other operational, legal, or regulatory reasons. Any changes will become effective upon posting of the updated Policy to the Platform, as indicated by the updated date at the top of this Policy.

Where required by applicable law, or where changes are material, we will provide you with advance notice of such changes using the contact information you have provided or through other appropriate means. Your continued access to or use of the Services following the effective date of any amendment constitutes your acknowledgement of the updated Policy.

We encourage you to review this Policy periodically to stay informed about how we collect, use, and protect your personal data. If you do not agree with any changes to this Policy, you should discontinue your use of the Services.

18. Contact Details

If you have any questions, concerns, or requests regarding this Policy or our personal data handling practices, or if you wish to exercise any of your rights described in Section 14, please contact us at:

COREACCESS SOLUTIONS S.A.

World Trade Center, 7th Floor, 53E Street

Marbella, Bella Vista, Panama City

Republic of Panama

Email: [Email]

We will endeavour to respond to all legitimate requests within a reasonable timeframe. In some cases, particularly where requests are complex or numerous, it may take longer to respond. We will keep you informed of any delays.

19. Complaints and Supervisory Authority

If you have a concern or complaint about how we handle your personal data and you are not satisfied with our response, you may have the right to lodge a complaint with the applicable data protection, privacy, or supervisory authority in your jurisdiction of residence.

We encourage you to contact us in the first instance using the details in Section 18, so that we have the opportunity to address your concern directly and in a timely manner.

The applicable supervisory authority will depend on your jurisdiction of residence and the nature of your complaint. We are not in a position to identify the applicable authority for every jurisdiction, and we encourage you to seek independent advice if you are unsure of the relevant authority in your jurisdiction.

Nothing in this Policy limits your right to lodge a complaint with a competent supervisory authority or to seek any other remedy available to you under applicable law.