

Blockchain.com Privacy Policy

Last Updated: 01 June 2026

1. GENERAL PROVISIONS

1.1. We are committed to safeguarding your privacy and ensuring the security of your personal data; therefore, we issue this privacy policy (Privacy Policy), which explains the manner in which we process your personal data, delineates the rights to which you are entitled, and provides additional information concerning the processing of your personal data.

1.2. This Privacy Policy clarifies the data processing activities undertaken by us when you visit or access our websites (<https://www.blockchain.com/>) or applications operated by us (together Platform), visit our social networking sites Instagram, Facebook, LinkedIn, Medium, X, YouTube (Social Accounts), order or use our services, including AI services and contact us by email, phone, or other electronic communication channels.

1.3. Blockchain's Platform and services are not directed to persons under the age of 18 or the age of majority as required by local laws, and we do not knowingly request or collect any information about persons under the age of 18 or the age of majority as required by local laws. If you are under the age of 18 or the age of majority as required by local laws, please do not provide any personal information through the Platform or Services. If an individual submitting personal information is suspected of being younger than 18 years of age or the age of majority as required by local laws, Blockchain will require the relevant individual to close his/her account, and will take steps to delete the individual's information as soon as possible.

1.4. In this Privacy Policy "personal data" (Personal Data) shall refer to any information or set of information from which we can directly or indirectly identify you, such as your name, surname, email address, telephone number, etc. For the purposes of this Privacy Policy, "You" shall denote a user of the Platform and its services, a visitor to the Social Accounts or an individual who communicates with us.

1.5. In processing Personal Data, we comply with the requirements of the General Data Protection Regulation 2016/679 (EU) (GDPR), which serves as the main standard. Additionally, we adhere to all applicable laws in various jurisdictions, including to the UK GDPR, US California Consumer Privacy Act (CCPA), Singaporean Personal Data Protection Act 2012, and Cayman Islands Data Protection Law. We also follow the instructions of the controlling authorities.

1.6. Should you utilize the Platform, its services, visit our Social Accounts, or contact us, and have provided consent to receive direct marketing communications, we consider that you have read and understood the Privacy Policy. If you do not agree with this Privacy Policy, you cannot use the Platform and our Social Accounts.

1.7. The Platform and Social Accounts may contain links to, for example, websites of our partners or other projects of ours. This Privacy Policy does not apply to such external websites. We encourage you to review the privacy policies of any third-party sites or platforms before disclosing any personal information or proceeding further.

1.8. This Privacy Policy is subject to change; therefore, we advise you to periodically visit the Platform to review the latest version of the Privacy Policy published.

2. WHO ARE WE?

2.1 Blockchain Account:* **

2.1.1 For UK, EEA, Switzerland and rest of the world residents: Blue Cube (Malta) Ltd., company number C 112722, address 171 Triq L- Ifran, VLT 1455 Valletta, Malta.

2.1.2 For Nigeria residents: BC Access (Nigeria) Limited, company number 7229704, Plot 9/10, Block 2, Oniru Chieftaincy Estate, P.O.Box 53197, Ikoyi-Lagos, Lagos, Nigeria.

2.1.3 For Ghana residents: BC Access (Ghana) Limited, company number CS197910825, 4 Momotse Avenue, Adabraka, Accra P. O. Box GP 1632, Accra, Ghana.

2.1.4 For #IM residents: Blue Cube Access (Global) Limited, company number C-57354, Unit 5, Long Stone House, Main Street, Charlestown, Nevis.

2.1.5 Blockchain (LT), UAB, company number 305048386, address Upės str. 23, LT-08128, Vilnius, the Republic of Lithuania, data about the company is being collected and stored in the Register of Legal Entities of the Republic of Lithuania.

2.2 De-Fi Wallet:* **

Blockchain.com (BVI) III Limited, company number 2088862, 2nd Floor Water's Edge Building, Wickhams Cay II, Road Town, Tortola VG1110, British Virgin Islands.

2.3 Staking Services:* **

Blockchain.com (Cayman) Limited, company number 384076, P.O. Box 144, Suite 3119, 9 Forum Lane, Camana Bay, George Town, Grand Cayman, KY1-9006, Cayman Islands.

2.4 Passive Rewards and Active Rewards:* **

Blockchain.com (BVI) Limited, company number 2086251, 2nd Floor Water's Edge Building, Wickhams Cay II, Road Town, Tortola VG1110, British Virgin Islands.

2.5 OTC Spot and Trade Execution Services* **

Blockchain.com (Singapore) Pte. Ltd., code 201817211W, 65 Chulia Street, #41-08, OCBC Centre, Singapore 049513.

* based on your country of residence which you disclosed to us as part of your onboarding process and/or services used, and further defined in the Blockchain.com User Agreement available at www.blockchain.com.

** to the extent the same is available to users based on their jurisdiction of residence from time to time.

We administer the Platform and provide services accessible through it.

3. HOW DO WE RECEIVE YOUR PERSONAL DATA?

3.1 We receive your Personal Data:

3.1.1. directly from You when You provide your Personal Data to us. For example, when You use the Platform and its services, make a payment, communicate with us by email or telephone, etc.;

3.1.2. when You use the Platform or Social Accounts. For example, We may record Your visit history on the Platform, purchases, IP address, service preferences, accessed URL links, etc.

3.1.3. from other parties, such as your service providers, payment institutions regarding payments made, public databases, etc.

3.2 When You provide Personal Data about yourself or others (e.g., about your employees, agents), You are responsible for the accuracy, completeness, and timeliness of such Personal Data, as well as for obtaining the necessary consent or informing the individual whose Personal Data is being provided to us. In certain cases, We may request confirmation from You that You have the right to provide us with Personal Data, for example, by completing registration forms.

4. WHAT PERSONAL DATA DO WE PROCESS ABOUT YOU?

4.1. We process your Personal Data for the following purposes and in accordance with the following terms and conditions:

Purposes of personal data processing	Processed personal data	Legal grounds for personal data processing
Creating and using an account on the Platform, and receiving other services provided via Platform, including AI services.	<p>Personal identification data: name, surname, date of birth, gender, citizenship, signature, government identifiers (government issued identity documents such as passport, national identification number, national identity card details, drivers' license numbers), photographs, and a video or voice recording of you, biometric data you provide to third parties who provide identify verification services to us, your status as a politically exposed person;</p> <p>Contact information: email address, phone number, address, country, region, proof of address;</p> <p>Employment information: job title, salary wage rate, and company, person that you represent (when</p>	<p>Consent of the data subject (Article 6(1)(a) and 9(2)(a) of the GDPR).</p> <p>The processing is necessary for the conclusion and performance of the contract (Article 6(1)(b) of the GDPR);</p> <p>The processing is necessary for compliance with a legal obligation imposed on the controller to ensure proper financial accounting (Article 6(1)(c) of the GDPR) in accordance with the Know Your Customer ("KYC") obligations under applicable laws and, in particular, regarding the compliance with Anti-Money Laundering laws and regulations.</p>

	<p>you represent a company or another person), relationship with the person represented;</p> <p>Authentication data: username, security questions, encrypted account passwords, biometric data you provide to third parties who provide identity verification services to us;</p> <p>Wallet information: wallet address, wallet ID, and other information related to integrations that you select;</p> <p>Account usage information: history, information on interactions with the Platform;</p> <p>Information on the services received via Platform, service-related communications and notifications;</p> <p>Information about the transactions you make on our services, such as the name of the recipient, and e-mail, time, location, transaction ID's, transaction amounts, wallet address, timestamps or transactions or events, bank account and/or credit card details, source of funds, account balances.</p>	
<p>Consultations on services available on the Platform and quality assurance.</p>	<p>If provided: name, surname, email address, phone number;</p> <p>Person represented (if you represent a company or another person), your relationship with the person represented;</p> <p>Subject and content of the communication (message, reply) and any data necessary to address quality issues;</p>	<p>Consent of the data subject (Article 6(1)(a) of the GDPR);</p> <p>The processing is necessary for the conclusion and performance of the contract (Article 6(1)(b) of the GDPR);</p> <p>The legitimate interests of the controller to provide information and to ensure</p>

	In the case of communication via social networks, we may collect publicly visible information from your account.	the quality of the service efficiently and effectively (Article 6(1)(f) of the GDPR).
Creation and execution of agreements necessary for service provision and Blockchain operations, other internal administration.	Name, surname, email address, phone number, position, workplace, represented person (when representing a company or another person), relationship with the represented person, individual activity data, other collaboration data.	The processing is necessary for the conclusion and performance of the contract (Article 6(1)(b) of the GDPR);
Managing payments, accounting, debt management.	<p>Name of the payer / person for whom the payment is made;</p> <p>Personal identification number (if applicable), government identifiers (government issued identity documents such as passport, national identification number, national identity card details, drivers' license numbers);</p> <p>Person represented (when representing a company or another person), relationship with the person represented;</p> <p>Address, email address, telephone number;</p> <p>Amount of the payment, date of the payment, number of the payer's account, payment institution, confirmation of payment by the collector of the contribution, payment card information, source of funding, source of wealth, account information, user ID and pay ID;</p> <p>Details of the arrears (date, amount, basis of the origin of the arrears, debtor passed on / unpassed to the debtor for collection).</p>	<p>The processing is necessary for the conclusion and performance of the contract (Article 6(1)(b) of the GDPR);</p> <p>The processing is necessary for compliance with a legal obligation imposed on the controller to ensure proper financial accounting (Article 6(1)(c) of the GDPR) in accordance with the laws on payments, tax, financial accounting and reporting and other legislation;</p> <p>The legitimate interests of the controller or third party to effectively manage financial operations and debts (Article 6(1)(f) of the GDPR).</p>

<p>Assessment and selection of candidates for the proposed job position.</p>	<p>Name, surname, email address, phone number, address, educational and activity data, content of the curriculum vitae, other information provided by the candidate necessary for selection/assessment.</p>	<p>The processing is necessary for the conclusion of the contract (Article 6(1)(b) of the GDPR) when you submit your candidacy for our proposed job position or the legitimate interests (Article 6(1)(f) of the GDPR);</p> <p>Consent of the data subject (Article 6(1)(a) of the GDPR).</p>
<p>Platform administration, development, assurance of security, fraud prevention.</p>	<p>IP address, device information, browser type and version, device type category and model, time zone setting and location data, language data, application version, browser type and version, device type category and model, time zone setting and location data, language data, application version and data collected by cookies (please consult our Cookie Policy), analytical data (such as visits, page views, searches, links clicked, and the date and time of those clicks), URL links directing to the Platform, and information about data changes.</p>	<p>Consent of the data subject (Article 6(1)(a) of the GDPR).</p> <p>The legitimate interests of the controller in ensuring the smooth functioning, development and security of the Platform (Article 6(1)(f) of the GDPR).</p>
<p>Managing Social Accounts.</p>	<p>Username, comments and shares on the post, information about clicks on “like” and “follow”, information about reactions to entries, photo, details of the message and the reply to the message (time of receipt, content, attachments), rating information, and any other information you provide.</p>	<p>Consent of the data subject (Article 6(1)(a) of the GDPR).</p>
<p>Conducting direct marketing campaigns, sending newsletters, conducting quality surveys for the improvement of the Blockchain’s services and activities.</p>	<p>Data used for sending newsletters and marketing: name, surname, email address, telephone number; preferences for the content of the newsletter, service usage data for personalized newsletters; URL links to the Platform, information</p>	<p>Consent of the data subject (Article 6(1)(a) of the GDPR).</p> <p>The legitimate interests of the controller to manage the mailing lists of news recipients, to analyse</p>

	about the recipients of the newsletters; data collected via advertising cookies.	aggregated marketing results, to resolve problems related to the provision of news (Article 6(1)(f) of the GDPR).
Publication and management of feedback regarding the Blockchain's activities.	The name, surname, email address, content of the feedback, submission date, social media account information, including a photograph, when the feedback is submitted via social media, provided by the person submitting the feedback.	Consent of the data subject (Article 6(1)(a) of the GDPR).
Public information about the Blockchain's activities.	Personal data, photographs, video material, excerpts from training content contained in publications, magazines, and other presented content.	Consent of the data subject (Article 6(1)(a) of the GDPR). The legitimate interests of the controller or third party to effectively manage electronic information delivery channels (Article 6(1)(f) of the GDPR).
Resolving disputes and claims.	Email address, content of the complaint / claim / proceeding, information related to the dispute / claim; Other data provided by the person: name, surname, phone number, address, job title, person represented (if You represent a company or another person), relationship with the person represented.	The processing is necessary for compliance with a legal obligation imposed on the controller (Article 6(1)(c) of the GDPR) in accordance with the laws on litigation and/or arbitration, as well as other legislation; Legitimate interests of the controller or of a third party to assert claims or defend their rights (Article 6(1)(f) of the GDPR).

4.2. You have the right to object to or withdraw your consent to the processing of your Personal Data at any time when such processing is based on consent.

4.3. In some cases, we may use the contacts you have provided to send you messages or call you in connection with our services. Such communications are essential for the proper provision of our services and are not considered promotional communications.

4.4. You have the right to amend and update the information we hold about You. In some cases, it is necessary for us to have accurate up-to-date information pertaining to You and We may request that You confirm the accuracy of information we hold about You. In providing services,

we may, in certain instances, employ automated decision-making based on data processing, for example, to comply with “Know Your Customer” obligations, ascertain your needs related to the service and their compliance with the requirements set by the service. Automated decision-making involves the processing of Personal data using, for instance, software code or an algorithm which does not require human intervention. We regularly review the automated decision-making methods we use to ensure their fairness, efficiency, and impartiality. You have the right to challenge the results of an automated decision – in such a case, your situation will be assessed by our specialist.

4.5. Personal data retention periods:

4.5.1 We retain your information as long as needed to provide our services, meet legal requirements, or protect our interests or others. Retention periods vary by country and depend on how the data is used. Factors influencing retention include the date of collection, its necessity for providing services, and legal requirements such as KYC or AML compliance, financial transactions, financial accounting, and other applicable regulations.

4.5.2 When processing data based on your consent, we shall do so for the duration of your consent. Should you withdraw your consent, we shall retain the data until the originally agreed upon period of consent expires.

4.5.3 Biometric data that you provide to vendors for identity verification purposes will be subject to those vendor’s retention policies.

4.5.4 For Social Accounts, data is stored according to their respective settings.

4.5.5 Platform data is stored as described in the Privacy Policy section “Cookies and other tracking technologies”.

4.5.6 Publicly disclosed data (in publications, magazines, etc.) are processed until the end of their public disclosure.

4.5.7 In line with these considerations, we delete information that is no longer needed for the above purposes when you close your account, or when you request deletion of your information.

5. SOCIAL ACCOUNTS

5.1. We post information regarding our Platform, activities, services offered, changes to said services, and other news on our Social Accounts. Additionally, we may post advertisements or communicate with you through them to respond to your inquiries.

5.2. It is important to bear in mind that users of Social Accounts are subject not only to this Privacy Policy, but also to the privacy policies, rules and terms of use of the operators of the social networks on which the Social Accounts are located. When you interact with us on the Social Accounts and provide certain information (for example, by messaging us and commenting on our posts), We may see public information about your profile (such as your name, image, email, etc.) depending on the privacy settings you have selected. This information, for example, a comment you have posted, may also be visible to other visitors to a particular Social Account, depending on the privacy settings You have selected.

6. HOW DO WE USE YOUR PERSONAL DATA AND WHAT PRINCIPLES DO WE ADHERE TO?

6.1. We respect Your privacy and only collect and process Personal Data that is necessary to achieve our stated purposes for processing Personal Data.

6.2. In processing your Personal Data, we shall:

6.2.1. comply with the requirements of applicable and valid legislation, including the GDPR;

6.2.2. process your Personal Data in a lawful, fair and transparent manner;

6.2.3. We collect your Personal Data for specified, clearly defined and legitimate purposes and We do not process it in a manner that is incompatible with those purposes, except to the extent permitted by law;

6.2.4. We take all reasonable steps to ensure that Personal Data which is not accurate or complete in relation to the purposes for which it is processed is promptly rectified, supplemented, its processing is suspended, or it is destroyed;

6.2.5. We retain them in a form which permits your identification for no longer than is necessary for the purposes for which the Personal Data is processed;

6.2.6. We do not provide Personal Data to third parties and will not disclose it other than as set out in the Privacy Policy or applicable law;

6.2.7. We ensure that your Personal Data is processed securely, by implementing technical and organizational security measures, and by restricting access to your Personal Data to those of our employees who need such access for the purposes of their job functions.

7. TO WHOM AND WHEN DO WE TRANSFER YOUR PERSONAL DATA?

7.1. We may transfer your Personal Data to processors or recipients who assist us in the performance of our activities such as our service providers, i.e. providers of marketing, advertising, newsletters services, providers of financial accounting, financial and payment services, providers of document management systems, accounting systems services, providers of IT solutions services, office software, data storage, management, exchange services, providers of cloud and hosting services, providers of KYC or AML services, providers of fraud prevention services, couriers, insurers, and suppliers of parts and materials.

7.2. To enable us to publish content on Social Accounts, We disclose data to the following operators of social networking platforms:

7.2.1. Meta Platforms Ireland Limited (Ireland) and Meta Platforms, Inc., (USA), (data is transferred in accordance with an adequacy decision issued by the European Commission; active participant of EU-U.S. Data Privacy Framework and Swiss-U.S. Data Privacy Framework);

7.2.2. Twitter International Unlimited Company (Ireland) and X Corp. (USA), (data is transferred in accordance with an adequacy decision issued by the European Commission; active participant of EU-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework and Swiss-U.S. Data Privacy Framework);

7.2.3. LinkedIn Ireland Unlimited Company (Ireland) and LinkedIn Corporation (USA) (data is transferred in accordance with an adequacy decision issued by the European Commission; active participant of EU-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework and Swiss-U.S. Data Privacy Framework);

7.2.4. YouTube Inc. (USA) (data transferred in accordance with the EU Standard Contractual Clauses approved by the European Commission);

7.2.5. Google Ireland Limited (Ireland) and Google LLC (USA) (data is transferred in accordance with an adequacy decision issued by the European Commission; active participant of EU-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework and Swiss-U.S. Data Privacy Framework);

7.2.6. Medium Corporation (USA) (data transferred in accordance with the EU Standard Contractual Clauses approved by the European Commission).

Given that Blockchain does not administer the aforementioned social networks listed above, but solely its own account on these social networks, You are invited to review the information regarding the storage of your personal data in the privacy documents of these respective social networks.

7.3. We may disclose data to law enforcement and pre-trial investigation authorities, courts and other dispute resolution authorities, as well as to other individuals or entities performing functions mandated by law, in accordance with the procedure stipulated by the legislation. We provide these entities with information that is required by law or as specified by the entities themselves.

7.4. We may also transfer data, if necessary, to companies that would buy or acquire our business or engage in joint activities or other forms of cooperation with us, as well as to companies established by us.

7.5. We generally process Personal Data within the EU / EEA, but in some cases your Personal Data may be transferred outside the EU / EEA. The transfer of your Personal Data outside the EU / EEA is based on:

7.5.1. a data processing or supply agreement that describes such transfer and includes Standard Contractual Clauses for international transfers; or

7.5.2. an adequacy decision adopted by the European Commission, which means that the European Commission has recognized the country in which the third party is established and / or carries on business as providing an adequate level of protection of personal data; or

7.5.3. a specific authorization by the data protection supervisory authority to carry out such transfer; or

7.5.4. your consent to the transfer of your Personal Data outside the EU / EEA.

8. WHAT RIGHTS DO YOU HAVE?

8.1. As a data subject, You may have the following rights in relation to your Personal Data depending on your jurisdiction:

8.1.1. to be informed about the processing of your Personal data and to have access to your Personal Data, i.e., to receive a notice confirming whether We are processing your Personal Data and, if We are, to request access to the data processed and the information relating to it;

8.1.2. to ask us to correct inaccurate or incorrect information We use or to supplement information where it is incomplete;

8.1.3. to ask us to erase information We hold about You where there is a basis for erasure (an exception to this right is provided for in point 8.9.);

8.1.4. to request us to restrict the processing of the information We hold about You where You contest the accuracy of the data or object to the processing of the data, You object to the erasure of your data which is unlawfully processed, or You need the data in order to assert, exercise, or defend legal claims;

8.1.5. to object to the use of your data where We process your data for our and / or third parties legitimate interests (including profiling, if we were to conduct such);

8.1.6. to request us to transfer / receive data that You have provided to us under a contract or consent and that We process by automated means in a commonly used electronic format;

8.1.7. to object to the application to You of a fully automated decision, including profiling, where such a decision may have legal consequences or a similar significant effect on You;

8.1.8. to withdraw the consents, You have given us to use information about You where We are using the data on the basis of your consent, including when we process Personal data for direct marketing purposes, as well as when we conduct profiling related to direct marketing;

8.1.9. to lodge a complaint with the relevant data protection supervisory authority.

8.2. We may refuse to fulfill your rights, except for the right to object to the processing of your Personal Data when it is processed based on consent, including consent for direct marketing, where We are not permitted to comply with your request under the GDPR.

8.3. If You wish to withdraw your consent for the processing of Personal data or to exercise any of your rights set out above, You may contact us by email at dpo@blockchain.com. In order to better understand your request, we may ask you to fill in the relevant request form, request a signed request with an advanced or qualified electronic signature, send the request by post or visit us in person.

8.4. For security reasons, in some cases we will only be able to process your request after verifying your identity. We may, therefore, ask you to prove your identity, for example by providing the document or other pertinent information.

8.5. You can exercise certain rights as a data subject by adjusting your account settings on the Platform or deleting your account yourself. However, by modifying your settings or deleting your account, You may lose some or all of the information stored therein.

8.6. We do not typically charge any fee for exercising your rights. However, the law permits us to charge a reasonable fee or to refuse to comply with your request if it is manifestly unfounded or excessive.

8.7. If you do not wish for your Personal data to be processed for direct marketing purposes, you can refuse such processing without specifying the reasons for refusal, by writing to the email address provided or in another manner indicated in the message provided to you (for example, by clicking the relevant link in the newsletter).

8.8. Upon receipt of your request or instruction regarding the processing of your Personal Data, We will provide You with a response within no later than 1 month from the date of the request and will execute the actions specified in the request or inform You why We refuse to do so. If necessary, the time limit may be extended by an additional 2 months due to the complexity and number of requests. In this case, we will notify you of the extension within 1 month of receiving the request.

8.9. If Personal Data is erased at your request, We may retain copies of the information as necessary to protect our legitimate interests and those of others, to comply with obligations of public authorities, to resolve disputes, to identify disturbances or to comply with agreements.

9. NEWSLETTER AND DIRECT MARKETING

9.1. We may send information regarding our activities, services (direct marketing communications) to your email address and/or telephone number, contact you via telephone if you have provided us with your consent to receive such information from us or if You or an organization you represent is a client of ours. Additionally, we may solicit your assistance in evaluating the quality of our performance and service.

9.2. To provide you with tailored newsletters, We may personalize direct marketing communications based on information about your use of our services. We utilize automated decision-making, including profiling, in order to provide you with tailored and effective direct marketing services based on your needs. For this purpose, we take into account your choices and preferences based on your behavior (for example, the type of regions you are interested in). The personalization solutions we use are solely intended to improve your experience. Should you choose not to receive our newsletters, this will not diminish your right to use our services and You will continue to receive the same quality of service.

9.3. If You no longer wish to receive direct marketing communications, You can unsubscribe using the method specified in the electronic communications (for example, by clicking on the “unsubscribe” link in the newsletter, etc.).

9.4. If You withdraw your consent, We will endeavor to cease sending You newsletters immediately; however, this may require some time, but never more than 10 business days. Given that our news campaigns are planned in advance, You may still receive our newsletters once more even after withdrawing your consent.

9.5. We may use your email address and telephone number for direct marketing purposes, to provide you with newsletters, offers, and information about similar services we offer that, in our opinion, may be of interest to you, as well as to inquire about the quality of our services and customer service, even without your consent if you are already our customer and have not objected to the use of your Personal data when you provided us with this information. Even if you have not expressed objection immediately, you can easily object to all or part of such Personal data processing activities at any time. You can do this:

9.5.1. by changing the subscription settings in your account on the Platform;

9.5.2. by informing us of your objection through the method specified in electronic communications and/or offers (for example, by clicking the “unsubscribe” link in the newsletter, etc.); or

9.5.3. by sending us a notification of objection to the email address specified in this Privacy Policy.

10. HOW DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

10.1. When you visit or access our websites or applications operated by us, or when you interact or engage with our content or use our services, we use (and authorize third parties to use) cookies and other tracking technologies.

10.2. Learn more about the way we process personal data when using cookies and other technologies in our Cookie Policy.

10.3. The Cookie Policy forms an integral part of our Privacy Policy.

11. HOW DO WE PROTECT YOUR PERSONAL DATA?

11.1. Your Personal Data is processed responsibly and securely, safeguarded against loss, unauthorized use and alteration. We have implemented both physical and technical measures to protect the information we collect from accidental or unlawful destruction, damage, alteration, loss, disclosure or any other unauthorized processing. The security measures for Personal Data shall be determined taking into account the risks involved in the processing of Personal Data. We follow industry-leading security standards and undergo independent external assessments to ensure the protection of user data. We are ISO 27001:2022 certified and have successfully completed SOC 2 Type 2 audits, demonstrating our commitment to the highest standards of information security and data protection.

11.2. We employ industry-standard security measures to protect your personal data. These measures include encryption, access controls, and regular security audits to prevent unauthorized access and ensure the integrity and confidentiality of your data.

11.3. Our employees are under a written obligation not to disclose or distribute your Personal Data to any unauthorized third party.

12. PRIVACY POLICY SUPPLEMENT FOR THE RESIDENTS OF THE UNITED STATES OF AMERICA

If you are a resident of the United States of America, you can learn more about how we use your information and your privacy rights by reviewing our Privacy Policy Supplement for Residents of the United States of America.

13. PRIVACY POLICY SUPPLEMENT FOR THE RESIDENTS IN NON-EU/UK/EEA/US JURISDICTIONS

If you are a resident in NON-EU/UK/EEA/US jurisdictions, please refer to the special provisions for respective jurisdictions:

British Virgin Islands	Residents of the British Virgin Islands (“BVI”) are protected under the Data Protection Act, 2021 (as amended). You have the right to access, correct, and delete your personal information. We implement stringent measures to protect your data and ensure that any transfers of your data outside the BVI are done with adequate safeguards.
Cayman Islands	As a resident of the Cayman Islands, your personal data is processed in accordance with the Data Protection Act, 2021 (revision). You have the right to access, correct, and delete your personal information, as well as to object to its processing under certain circumstances. We ensure that any transfer of your data outside the Cayman Islands is conducted with appropriate safeguards to maintain its protection.
Ghana	As a resident of Ghana, your personal data is processed in accordance with the Data Protection Act, 2012 (Act 843). You have the right to access, correct, and delete your personal information, as well as to object to its processing in certain circumstances. We ensure that any transfer of your data outside Ghana is carried out in compliance with applicable legal requirements and subject to appropriate safeguards to ensure the continued protection of your personal data.
Nevis	Residents of Nevis have rights under applicable privacy laws, including the right to access, correct, and delete their personal data. We take all necessary steps to protect your information and ensure that any transfers of your data outside Nevis comply with relevant data protection regulations, maintaining the privacy and security of your data.
Nigeria	As a resident of Nigeria, your personal data is processed in accordance with the Nigeria Data Protection Act, 2023. You have the right to access, correct, restrict, and delete your personal information, as well as to object to its processing in certain circumstances, data portability and right to be subjected to automated decision making. We ensure that any transfer of your data outside Nigeria is carried out with appropriate safeguards to maintain its protection.
Singapore	For residents of Singapore, we process your personal data in compliance with the Personal Data Protection Act (as amended) (PDPA). You have the right to access, correct, and request the withdrawal of consent for the use

	of your personal data. Data transfers outside Singapore are carried out in accordance with the PDPA, ensuring that your information remains protected.
--	--

14. CONTACT US

If you have any questions (or comments) concerning this Privacy Policy, you are welcome to contact us through the following contact details: dpo@blockchain.com

If you have any questions or complaints about our processing of your personal data, please first contact us directly at the contacts specified in the Privacy Policy. We will make our best effort to reply within a reasonable timeframe and to answer your questions or to solve incurred problems. Please feel free to reach out to us at any time - dpo@blockchain.com

If you are unsatisfied with our response, you can reach out to the applicable data protection authority:

Information and data protection commissioner, Floor 2, Airways House, Triq Il-Kbira, Tas-Sliema SLM 1549, +356 2328 7100, idpc.info@idpc.org.mt, <https://idpc.org.mt/>

Nigerian data protection commission, website available at <https://ndpc.gov.ng/>

Ghana Data Protection Commission, website available at <https://www.dataprotection.org.gh/>

Cayman Islands - The Office of the Ombudsman, website available at <https://ombudsman.ky/make-a-complaint>

Singaporean Personal Data Protection Commission PDPC, website available at <https://www.pdpc.gov.sg/complaints-and-reviews/report-a-personal-data-protection-concern/personal-data-protection-complaint>

The State Data Protection Inspectorate of Lithuania (Valstybinė duomenų apsaugos inspekcija, website available at <https://vdai.lrv.lt/>).

15. CHANGES TO PRIVACY POLICY

We regularly review this Privacy Policy and reserve the right to modify it at any time in accordance with applicable laws. Any changes and clarifications will take effect immediately upon their publication on our website. Please review the Privacy Policy from time to time to stay updated on the changes.

BLOCKCHAIN.COM
PRIVACY POLICY SUPPLEMENT FOR THE RESIDENTS OF THE UNITED STATES
OF AMERICA

1. GENERAL PROVISIONS

1.1. This Privacy Policy Supplement for Residents of the United States of America (“US Privacy Supplement”) is for residents of the United States of America, and describes how we collect, use, share and protect your personal information when you use our Platform.

1.2. This US Privacy Supplement supplements the transparency information provided in our Privacy Policy, because as a resident of the United States of America, you are afforded a range of data protection and privacy rights under various federal (including but not limiting to the Federal Trade Commission Act (FTC Act), the Gramm-Leach-Bliley Act (GLBA)) and state laws (including, but not limiting to California Consumer Privacy Act (as amended) (“CCPA”)) (together “US Privacy Laws”). These rights aim to ensure transparency, control, and security regarding the processing of your personal data.

1.3. Any terms defined in the CCPA or GLBA have the same meaning when used in this US Privacy Supplement.

2. COLLECTION, DISCLOSURE, SELLING OR SHARING OF PERSONAL INFORMATION

2.1. Blockchain.com collects the personal information specified in Section 4 of the Privacy Policy, either directly from you or from the sources listed in Section 3 of the Privacy Policy. We use and/or share personal information to create, develop, operate, deliver, and improve our services on the Platform, to communicate with you, to ensure the safety, security and integrity of our services, and for the business and commercial purposes as outlined in our Privacy Policy.

2.2. When you visit or access our websites or applications operated by us, or when you interact or engage with our content or use our services, we use (and authorize third parties to use) cookies and other tracking technologies. Learn more about the way we process personal data when using cookies and other technologies in our Cookie Policy.

2.3. In the preceding 12 months, Blockchain has shared to advertisers, ad networks, advertising partners, and advertising measurement providers, pursuant to written contracts that contain terms required by US Privacy Laws, the following categories of personal information:

2.3.1. Identifiers including, device identifiers, IP addresses, browser cookies, and other unique online identifiers;

2.3.2. Professional or employment related information;

2.3.3. Commercial information, such as transaction information and transaction history;

2.3.4. Internet activity information including data about a consumer’s interaction with our websites, application, service, or advertisement;

2.3.5. User Profile information including email address and general location information, such as device location and IP location;

2.3.6. Inferences drawn from Personal Information, including preferences, interests, and other data used to personalize a consumer's experience.

2.4. These categories are each shared for cross contextual behavioral advertising purposes, to target ads, and to provide analytics and reporting related to the effectiveness of advertising.

2.5. In an increasing number of US States, you can request that Blockchain.com not sell your personal information, share it with third parties for cross-context behavioral advertising purposes, or process it for targeted advertising purposes. For information about how to exercise your rights to opt-out, and to exercise that right, you can opt out of certain forms of on-line sale, sharing, or targeted advertising by turning off certain types of cookies and tracking tools by interacting with the cookie banner upon your first visit to Blockchain.com website or contacting us dpo@blockchain.com.

2.6. While many browsers permit you to send a signal about your Do Not Track ("DNT") preferences, we do not respond to DNT signals sent from browsers.

2.7. Please be aware that certain sharing of your Personal Information, such as disclosures of that Information to "Service Providers" as that term is defined and in accordance with CCPA, or for certain business operations of <https://www.blockchain.com/>, are not considered "sale" of Personal Information.

2.8 Additionally, we engage third-party providers to verify your identity, including for fraud prevention purposes and to comply with our legal obligations. These third parties may process and retain your biometric data to provide these services to us. For more information about how these third parties collect and use your biometric data, and how long they retain this information, you may refer to the Veriff Privacy Notice and Sumsu Privacy Notice.

2.9. Additional GLBA disclosures notice. GLBA requires us to tell you how we collect, disclose, and protect your personal information.

Financial companies choose how they disclose your personal information. Under the GLBA you have the right to limit some, but not all, sharing of your personal information. All financial companies need to disclose customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information, the reasons we choose to share, and whether you can limit this sharing:

Reasons we can share your personal data	Do we share?	Can you limit this sharing?
For our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations	Yes	No
For our marketing purposes – to offer our products and services to you	Yes	No

For joint marketing with other financial companies	N/A	N/A
For our affiliates' everyday business purposes – information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes – information about your creditworthiness	N/A	N/A
For our affiliates to market to you	Yes	Yes
For non-affiliates to market to you	N/A	N/A

When you are no longer our customer, we continue to share your information as described in this notice.

GLBA gives you the right to limit only:

- sharing for affiliates' everyday business purposes - information about your creditworthiness;
- affiliates from using your information to market to you;
- sharing for non-affiliates to market to you.

*Affiliates: companies related by common ownership or control. They can be financial and nonfinancial companies. Our affiliates include companies within Blockchain.com Group.

**Non-affiliates: companies not related by common ownership or control. They can be financial and nonfinancial companies. Non-affiliates we may share your information with listed in Section 7 of the Privacy policy. We do not share with non-affiliates so they can market to you.

***Joint marketing: a formal agreement between non-affiliated financial companies that together market financial products or services to you. Blockchain.com does not jointly market.

3. PRIVACY RIGHTS AND EXERCISING YOUR RIGHTS

3.1. You may be entitled to the following privacy rights listed below based on various state privacy laws, including if you are a resident of California, Colorado, Connecticut, Florida, Oregon, Texas, Utah, and Virginia:

3.1.1. Right to Know: You can request information about the categories and specific personal information that a company has collected about you.

3.1.2. Right to Access Information about Data Sharing: You have the right to limit the use and disclosure of your sensitive personal information to only those purposes necessary for the provision of goods or services, as described in the law;

3.1.3. Right to Correct: You have the right to request that a business correct any inaccurate personal information it has collected about you;

3.1.4. Right to Opt-Out: You can opt-out of the sale of your personal data to third parties.

3.1.5. Right to Deletion: You have the right to request the deletion of personal data that a company holds about you, with certain exceptions.

3.1.6. Right to Non-Discrimination: Companies cannot discriminate against you for exercising your CCPA rights, such as denying services or charging different prices;

3.1.7. Right to Data Portability: You have the right to receive your personal information in a portable and readily usable format that allows you to transmit the data to another entity without hindrance.

3.2. At Blockchain.com, we are committed to upholding and executing these rights. We actively engage in protecting your personal information through robust security measures, transparent data processing practices, and by providing you with the necessary tools and resources to exercise your privacy rights effectively.

3.3. You or an authorized agent can submit a request to exercise the rights applicable to you through our dpo@blockchain.com.

4. SECURITY MEASURES

4.1. We employ industry-standard security measures to protect your personal data. These measures include encryption, access controls, and regular security audits to prevent unauthorized access and ensure the integrity and confidentiality of your data. You can find more information on our security measures in Section 11 of the Privacy Policy.

4.2. We are committed to addressing your concerns and ensuring that your data is handled in compliance with applicable laws.

5. CHILDREN'S ONLINE PRIVACY PROTECTION ACT

5.1. Blockchain.com complies with the Children's Online Privacy Protection Act COPPA, which requires the consent of a parent or guardian for the collection of personally identifiable information from children under 13 years of age. Our products and services are not directed to persons under the age of 18 and Blockchain.com does not knowingly collect, use or disclose personal information from children under 18, or equivalent minimum age in the relevant jurisdiction, without verifiable parental consent. However, it is possible that we may inadvertently receive information pertaining to children under 18. If you believe that we have received information about your child that is under the age of 18, please do not hesitate to notify us at dpo@blockchain.com. When we receive your notification, we will obtain your consent to retain the information or will delete it permanently.

6. CHANGES TO US PRIVACY SUPPLEMENT

6.1. We regularly review this US Privacy Supplement and reserve the right to modify it at any time in accordance with applicable laws. Any changes and clarifications will take effect immediately upon their publication on our website. Please review the US Privacy Supplement from time to time to stay updated on the changes.