Privacy Policy

Introduction

This Privacy Policy (this "**Policy**") explains how Horus Research LLC (the "**Company**", "**we**", "**us**", "**our**") collect, use, and process your Personal Data (as defined herein) when you ("**you**", "**your**", "**user**") use the Services as defined in our Terms of Service), and any communications that we have with, or messages that we send to, you, or any transactions that we have with you (jointly called in this Privacy Policy, the "**Services**").

By continuing your interactions with us, such as by submitting information to us, or using our Services, you confirm that you understand and consent to the collection, use, disclosure, and processing of your Personal Data (or the Personal Data of any individual you provide) as described in this Policy.

For the purposes of the General Data Protection Regulation of the European Union (EU), and the data protection laws of other relevant jurisdictions where users are located (collectively, the "**Data Protection Laws**"), the Company is the data controller (i.e., the company who is responsible for, and controls the processing of, your Personal Data, as defined herein).

Please note that we take the protection of personal data very seriously.

IF YOU DO NOT AGREE WITH ANY PART OF THIS POLICY, THEN PLEASE DO NOT SUBMIT INFORMATION TO US AND DO NOT USE ANY OF OUR SERVICES.

From time to time, we may revise or amend this Privacy Policy to reflect changes in law, our Personal Data collection and use practices, the features of the Services, or advances in technology. This Policy does not cover the practices of entities we do not own or control, or people we do not manage.

By accessing and/or using our Services, you shall be deemed to consent to all terms and conditions in this Policy.

If you have any questions or requests regarding this Privacy Policy, please contact our Data Protection Officer at the contact details provided below (at the end of this Privacy Policy).

The terms used in this Privacy Policy shall have the same meanings as in the Terms of Service except as otherwise provided herein.

Personal Data that we may collect about you

From time to time, we may directly or indirectly collect or ask you to provide the following information:

a) your name;
b) your email address;

c) your social media and/or instant messaging application account name and other public information;
d) your geographic location, transaction location, and IP addresses that you use when you use our Services; and/or
e) information about your device and its software, such as your IP address, browser type, Internet service provider, platform type, device type, operating system, date and time stamp, a unique ID (that allows us to uniquely identify your browser, mobile device, or your account), and other similar information.

We may directly or indirectly collect or ask you to provide the following information (if any):

a) the public key of your Wallet (wallet address);
b) information on transactions made through your Wallet;
c) full name, date of birth, gender, country of residence, username, passwords, tax numbers, and data included in government-issued identification documents;
d) financial information, sources of wealth or funds or income, level of activity anticipated, distributed ledger network wallet addresses;
e) personal Documents such as government-issued IDs, passport, bank statements, utility bills, internet bills, income, account balances, financial transaction history, credit history, tax information, and credit scores, and other forms of identification, address verification and source of funds and wealth verification;
f) corporate information such as legal entity name, doing business as name, legal domicile, fiscal domicile, object;
g) corporate documents such as certificate of registration, constitution, memorandum & articles of association, bylaws, statues, incumbency certificate, register of directors, register of shareholders, register of authorized signatories, registry excerpts, financial statements;
h) contents of the message and/or attachments you may send other users or us;
i) on whether you meet the criteria for particular activities offered within the Services;
j) on your ownership of virtual assets;
k) on whether a user invited third parties to use the Services;
l) on decisions you may make during the usage of the Services;
m) on whether you applied for Services usage previously;
n) on your public posts on social networks;
o) that you explicitly share with us to use the Services.

We may also receive information from the following sources:

a) from third parties from time to time (for example, partners, sub-contractors in KYC, AML, technical, payment, and delivery services, advertising networks, analytics providers, search information providers, virtual asset service providers and credit reference agencies) who may provide us information about you;
b) if you choose to link our Services to a third-party account (e.g. for authentication purposes to use our Services, such as Apple ID or Google Account) , we may receive information about that account, such as your authentication token from a third-party account, to authorize linking. Please note that the information we may receive is governed by the privacy settings, policies, and/or procedures of a third party;

c) from advertising networks, analytics providers and search information providers may provide us with pseudonymised information about you, including confirmation of how you found our Services;
d) we may also collect information from social media platforms that share information about how you interact with our social media content; and
e) we may receive technical data related to your activities within the Service automatically from your browser, our servers, and our systems.

Subject to the applicable Data Protection Laws, in some jurisdictions and depending on particular circumstances, all or some of the above information and data can be considered your personal data (all the above and any other personal data as defined under Data Protection Laws, or as mentioned in this Policy, collectively referred to as the "**Personal Data**").

We may monitor, record, and store your Personal Data in order to protect your safety or the safety of other users, comply with relevant laws, to assist with regulatory or law enforcement efforts, to protect and defend our rights and property, or for other reasons relating to our provision of the Services. By using the Services, you consent to the recording, storage, and disclosure of such information you send or receive for these purposes.

We may need your Personal Data to provide the Services to you and/or perform our contractual obligations towards you. You can always refuse to provide your Personal Data. However, without providing Personal Data, we may not be able to provide you with the Services you are intending to receive.

Distributed Ledger Technologies and Data Protection Laws

To provide some of the Services, the Company may use distributed ledger technologies ("**DLT**"). Please find below the most crucial issues you should know about these technologies.

A blockchain is often structured as a chain of blocks. A single block groups together multiple transactions and is added to the existing chain of blocks through a hashing process. A hash function (or hash) provides a unique fingerprint that represents information as a string of characters and numbers. It is a one-way cryptographic function, designed to be impossible to revert. The blocks themselves are made up of different kinds of data, which includes a hash of all transactions contained in the block (its fingerprint), a timestamp, and a hash of the previous block that creates the sequential chain of blocks. Some of this data can be qualified as personal data in some jurisdictions.

Because blocks are continuously added but never removed, a blockchain can be qualified as an append-only data structure. Cryptographic hash-chaining makes the log tamper-evident, which increases transparency and accountability. Because of the hash linking one block to another, changes in one block change the hash of that block, as well as of all subsequent blocks. It is because of DLT's append-only nature that the modification and erasure of data cannot straightforwardly be implemented. DLT freezes facts (information entered can, as a general rule, not be changed) and the future (smart contracts' execution cannot be halted

even where parties change their mind). Blockchains are usually deliberately designed to render the (unilateral) modification of data difficult or impossible.

Whereas Data Protection Laws in some jurisdictions require that Personal Data that is processed be kept to a minimum and only processed for purposes that have been specified in advance, these principles can sometimes be hard to apply to blockchain technologies. Distributed ledgers are append-only databases that continuously grow as new data is added. Such data is replicated on many different computers. It is moreover can be unclear how the 'purpose' of personal data processing ought to be applied in the blockchain context, specifically whether this only includes the initial transaction or whether it also encompasses the continued processing of Personal Data (such as its storage and its usage for consensus) once it has been put on-chain.

In public and permissionless blockchains, anyone can entertain a node by downloading and running the relevant software – no permission is needed. In such an unpermissioned system, there are no identity restrictions for participation. Permissionless blockchains rely on open-source software that anyone can download to participate in the network. Blockexplorers are a form of a search engine that moreover make such blockchain data searchable to anyone. The public auditability of these ledgers enhances transparency but minimizes privacy.

Regarding DLT usage, we should warn you about the following:

a) subject to applicable laws, data typically stored on a distributed ledger, such as public keys and transactional data, generally can be qualified as personal data for the purposes of Data Protection Laws;
b) Personal Data that has been encrypted or hashed can also be qualified as personal data;
c) usually (not always), we keep Personal Data private from the blockchain in an “off-chain” data store, with only its evidence (cryptographic hash) exposed to the chain;
d) we believe that you are sufficiently sophisticated with regard to distributed ledger technologies, in general, to be able to safeguard yourself from the relevant risks.

If you believe that data transferred by you to a distributed ledger likely does qualify as Personal Data for Data Protection Laws purposes, we appreciate your position and can not recommend using our Services. Otherwise, there can be further difficulties in the execution of all rights granted by Data Protection Laws in your jurisdiction.

Data transferred to a distributed ledger can be considered as Personal Data which are manifestly made public by you.

How we use your Personal Data

To the fullest extent permitted under applicable under Data Protection Laws, we use your Personal Data to:

a) provide, troubleshoot, and improve the Services (using our own systems and third-party service providers, when applicable);
b) analyze usage and performance of the Services;
c) communicate with you, including without limitation, to inform you of updates to the Services, our terms of use or other contractual arrangement that applies to our relationship with you (the "**Contracts**"), and/or this Policy;
d) comply with applicable Know Your Customer, Anti-Money Laundering, Counter-Terrorism Financing, and Anti-Corruption laws and regulations;
e) deliver advertising, marketing or information which may be useful to you;
f) respond to your inquiries and requests;
g) perform market and customer researches;
h) investigate and/or prevent suspected fraud, other criminal activities, or intellectual property infringement; prevent and detect abuse to protect the security of the users, the Services, and others;
i) comply and enforce applicable regulations and agreements, including enforcing the Contracts or other legal rights, or as may be required by applicable laws and regulations or requested by any judicial process or governmental agency;
j) operate the Services;
k) develop aggregate analysis and business intelligence that enable us to protect, make informed decisions, and report on the performance of the Services;
l) disclose data to potential acquirers of the project, including legal advisors and auditing service providers in case of a merger, acquisition, or selling the whole or part of the Company or the Services;
m) disclose data to our service providers, including the transfer of your Personal Data;
n) deliver joint content and services with third parties with whom you have a separate relationship (for example, social media providers); and
o) in addition to the legal and commercial uses listed above, we may be required to provide any and all of your Personal Data to governmental authorities as necessary to comply with the law. To the extent required by Data Protection Laws, or where we have a legitimate and lawful purpose for doing so, we may retain information about you.

We may process your Personal Data for other purposes, provided that we disclose the purposes and use to you at the relevant time and that you either consent to the proposed use of the personal data, other legal grounds exist for the new processing purposes, or the new purpose is compatible with the original purpose brought out above.

The Services may contain technology that enables us to:

1. Check specific information from your device or systems directly relevant to your use of the Services, applications or Services against our records to make sure the Services services are being used in accordance with our end-user agreements and to troubleshoot any problems;
2. Obtain information relating to any technical errors or other issues with our Services;
3. Collect information about how you use the features of our Services; and
4. Gather statistical information about the operating system and environment from which you access our Services.

If you become a follower of the Company in social networks, the processing of Personal Data will be governed by the policies of the Social Network, as well as by their terms of use, privacy policies and regulations that belong to the social network that corresponds in each case and that you have previously accepted.

The Company will treat your Personal Data in order to correctly manage your presence in the social network, inform you of the Company activities, Services, as well as for any other purpose that the rules of the social networks allow.

In no case will the Company use the profiles of followers in social networks to send advertising individually.

Legal basis for processing Personal Data

We collect your Personal Data for the following purposes:

1. Where necessary to perform any contract we enter into, or have entered into, with you to provide Services or provide access to our Services;
2. Where necessary for our legitimate business interests (or those of a third party) when your interests and fundamental rights do not override those interests;
3. Where necessary to protect the vital interests of any individual, when your interests and fundamental rights do not override those interests;
4. Where we need to comply with a legal or regulatory obligation in any relevant jurisdiction; and
5. For any other purpose, based on your explicit consent, for instance, for marketing, customer support, technical support, which can be revoked at any time; and we will stop processing your data for that purpose.

Your legal rights

Subject to applicable law and this Policy, you may have the following rights:

a) Right to access: you have the right to obtain confirmation that your Personal Data are processed and to obtain a copy of it as well as certain information related to its processing;
b) Right to rectify: you can request the rectification of your Personal Data which are inaccurate and also add to it;
c) Right to delete: you can, in some cases, have your Personal Data deleted;
d) Right to object: you can object, for reasons relating to your particular situation, to the processing of your data. You may ask us to restrict the processing of your Personal Data;
e) Right to limit the processing: in certain circumstances, you have the right to limit the processing of your Personal Data;
f) Right to portability: in some cases, you can ask to receive the Personal Data that you have provided to us in a structured, commonly used, and machine-readable format or, when this is possible, that we communicate your data on your behalf directly to another data controller;

g) Right to withdraw your consent: for processing requiring your consent, you have the right to withdraw your consent at any time. Exercising this right does not affect the lawfulness of the processing based on the consent given before the withdrawal of the latter, nor will it affect the processing of your Personal Data conducted in reliance on lawful processing grounds other than consent;
h) Right to define the instructions relating to the use of your Personal Data post-mortem: you have the right to define instructions relating to the retention, deletion, and communication of your data after your death;
i) Right to non-discrimination: you have the right not to receive discriminatory treatment as a result of your exercise of rights conferred by laws applicable in your jurisdiction; and
j) Right to lodge a complaint to the relevant data protection authority: procedure depends on your jurisdiction and is subject to local regulations. For more information, please contact your local data protection authority.

The exercise of these rights is personal and therefore must be exercised directly by the interested party, requesting it directly to the Company, which means that any user, subscriber or collaborator who has provided their Personal Data at any time can contact the Company and request information about the data that it has stored and how it has been obtained, request the rectification of the same, request the portability of your Personal Data, oppose the processing, limit its use or request the cancellation of that data in Company's files.

If you wish to exercise any of the rights set out above, please contact our Data Protection Officer at the contact details set out below. When applicable, and subject to your country of residence or domicile, you may be charged with a reasonable fee for our processing of access requests, but not for processing a correction. Please note that in some cases we may reject requests for certain reasons (for example, if the request is unlawful or if it may infringe on the rights of others or if the request is clearly unfounded, repetitive or excessive).

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. However it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

For the avoidance of doubt, when we collect Personal Data for a purpose based on your explicit consent, you may withdraw such consent at any time, and at such point, we will stop processing and collecting your Personal Data for such purpose.

Personal Data Transfer / Sharing

The Company's authorized personnel, including but not limited to our Data Protection Officer, shall have access to your Personal Data on a need-to-know basis. Our authorized personnel

are bound to confidentiality and non-disclosure agreements, and subject to strict company policies related to the access and use of the data.

We may share Personal Data only as described below and with the subsidiaries or affiliates of the Company that are either subject to this Policy or follow practices at least as protective as those described in this Privacy Policy.

We may contract or employ companies and individuals to perform certain functions, examples may include analyzing data, providing marketing assistance, processing payments, transmitting content, and providing KYC/AML solutions. These third-party service providers only have access to personal data needed to perform their functions but may not use it for other purposes. Further, they must process the Personal Data in accordance with the relevant data sharing agreements which incorporate this Policy, and only as permitted by applicable Data Protection Laws.

Certain of your Personal Data may be shared with other users as part of the normal operation of the Services.

We may, from time to time, expand or reduce the Services, which may involve the transfer of certain divisions to other parties, and the data we process, where relevant, may be transferred to such third parties.

We may also share information to

a) satisfy any applicable law, regulation, legal process, or governmental request;
b) enforce this Policy and our Contracts, including investigation of potential violations hereof or thereof;
c) detect, prevent, or otherwise address fraud, security, or technical issues;
d) respond to your requests; or
e) protect our rights, property or safety, our users and the public. This may include exchanging information with companies and organizations for various purposes.

We may also share personal data when we do a business deal, or negotiate a business deal, involving the sale or transfer of all or a part of our business or assets. These deals can include any merger, financing, acquisition, or bankruptcy transaction or proceeding.

We may also share Personal Data for legal, protection, and safety purposes or to comply with laws.

We may engage from time to time to third-party service providers to assist the Company with the implementation of our KYC/AML & CTF Policy as well as the compliance with applicable Know Your Customer, Anti-Money Laundering, Counter-Terrorism Financing, and Anti-Corruption laws and regulations. Where applicable, we will enter into a data processing agreement with these third-parties to ensure data security and protection of your Personal Data against data breaches. Such data processors will only process your Personal Data to the extent required for the provision of services for which they are engaged.

We may share Personal Data with those who need it to do work for us. These recipients may include third party companies and individuals to administer and provide the Service on our

behalf (such as customer support, hosting, email delivery and database management services), as well as lawyers, bankers, auditors, and insurers.

The Company may transfer your data outside of the European Economic Area or to locations that may have different Data Protection Laws to your jurisdictions or no data protection laws. The Company puts in place reasonable technical, organizational, and contractual safeguards (including Standard Contractual Clauses, if applicable) to ensure that such transfer is carried out in compliance with applicable Data Protection Laws, except where the country to which the data is transferred has already been determined by the European Commission to provide an adequate level of protection.

We may use industry-standard data analytics tools claimed to be GDPR-compliant and CCPA-compliant.

For any other purpose than those stated above, we do not share, rent, or sell your Personal Data with other organizations without your express consent, except as described in this Policy.

Personal Data Retention

We will retain your Personal Data for as long as it is necessary for the purposes of performing a contract, comply with our legal and regulatory obligations, protect our legitimate interests. and for the purposes of Know Your Customer, Anti-Money Laundering, Counter-Terrorism Financing, and Anti-Corruption.

We reserve the right to retain your Personal Data for the aforementioned purposes, troubleshoot problems, assist with any investigation, enforce our Contracts or any other contract that we entered into with you, and other actions permitted by law; and for the purposes of preventing fraud, legal proceedings, complaints and disputes for as long as this is necessary to protect our legitimate interests, if we believe there is a prospect of litigation/dispute in respect to our relationship with you.

To determine the appropriate retention period for your Personal Data, we consider the purposes for which we process your Personal Data, the applicable legal requirements, and other legitimate interests.

We will retain your Personal Data for as long as it is necessary for the purposes of performing a contract, comply with our legal and regulatory obligations, and protect our legitimate interests. Specifically, we reserve the right to retain your Personal Data for the purposes of complying with applicable Know Your Customer, Anti-Money Laundering, Counter-Terrorism Financing, and Anti-Corruption laws and regulations for a period of at least seven (7) years, and for the purposes of legal proceedings, complaints and disputes for as long as this is necessary to protect our legitimate interests.

Personal Data Security

To protect your Personal Data, the Company takes all reasonable precautions and follows the best practices of the industry to prevent the loss, misuse, improper access, disclosure, alteration or destruction of the same.

In addition to the purposes described in this section, we may also use information we gather to deliver targeted and interest-based advertising, marketing (including in-product messaging) or information to you which may be useful, based on your use of the Services or any other information we have about you (depending on the Services, you may able to configure these features to suit your preferences).

We have implemented appropriate technical and organizational security measures designed to protect the security of any Personal Data we process. However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be entirely secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security, and improperly collect, access, steal, or modify your information. The transmission of Personal Data to and from our Services is at your own risk. You should only use the Services within a secure environment. We do not assume responsibility for the information you submit to or receive from us or for any unauthorized access or use of that information, and we cannot and do not guarantee the security of any information transmitted by you to us or vice versa. You agree not to hold us responsible for any loss or damage incurred as a result of any unauthorized access, modification, interception, destruction or use of the information you submit to or receive from us through the Internet. In the event of a data breach, we will notify you as soon as practicable as required by applicable law.

Content from other Services

The Services may include embedded content (for example, videos, images, articles, etc.). The embedded content of other internet websites ("**Third-Party Sites**") behaves in exactly the same way as if you had visited other internet websites.

These Third-Party Sites may collect data about you, use cookies, embed an additional third-party tracking code, and monitor your interaction using this code.

Please be aware that we are not responsible for the content or privacy practices of the Third-Party Sites. You acknowledge that we do not control how these Third-Party Sites collect, use and share your personal information and you further acknowledge that these Third-Party Sites fall outside the scope of this Privacy Policy and are governed by their own respective privacy policies. We are not responsible for the activity or content of any Third-Party Sites. We encourage our Users to be aware when they leave our site and to read the privacy statements of any other site that collects personally identifiable information.

Minors

The Services are not directed to children under the age of eighteen, and the Company will never knowingly collect Personal Data from children under the age of eighteen. If you are

under the age of eighteen, you must ask your parent or guardian for permission to use our Services.

Cookies

Our Services use cookies. By accessing our Services we will inform you, through a pop-up banner, of our use of cookies.

1. About cookies

Cookies are files, often with unique identifiers, that web servers send to Internet browsers and can then be sent back to the server each time the browser requests a page from the server.
Web servers use cookies to identify and track users while browsing the different pages of Services, as well as to identify users returning to Services.

Cookies can be “persistent” cookies or “session cookies”. A persistent cookie consists of a text file sent by a web server to an Internet browser, which is stored by the browser and remains valid until the defined expiration date (unless the user deletes it before the expiration date). On the other hand, a session cookie expires at the end of the user's session, when the Internet browser is closed.

2. Cookies from the Services

On our Services, including our Website, and mobile applications, we use session and persistent cookies.

We will send you the following cookies:

a. Session Cookies
b. Google Analytics: This cookie allows us to identify unique users, unique sessions, regulate the rate of requests and store information about user sessions and campaigns.

Cookie 1 is a session cookie, while Cookie 2 is a persistent cookie.

3. How we use cookies

Cookies do not contain personally identifiable information, but we have the possibility of linking the Personal Data we store about you with the information obtained and stored from cookies.
We use the information we obtain from the use of our cookies for the following purposes:

a. Recognize your computer when you access and/or use our Services.
b. Improve the usability of the Services.
c. Analyze the use of our Services.
d. Manage the Services.
e. Third party cookies

When you use the Services, you may also be sent third-party cookies.

Our service providers can send you cookies. They use the information they obtain through their cookies for the following purposes:

a. Track your browser on different Services.
b. Create a profile of your Internet browsing.
c. Select specific ads that may be of interest.

4. Deletion and blocking of cookies

You can, at any time, restrict, block or delete cookies from the Services. To do this, you must modify the configuration of your browser regarding the use of cookies through the “Preferences”, “Options” or “Tools” menu (the name of the menus or the procedure to access the cookie options vary depending on the browser used). Most browsers allow you to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser, and from version to version. You can however obtain up-to-date information about blocking and deleting cookies via these links:

- https://support.google.com/chrome/answer/95647 (Chrome);
- https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-Services-preferences (Firefox);
- https://help.opera.com/en/latest/security-and-privacy/ (Opera);
- https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies (Internet Explorer);
- https://support.apple.com/en-gb/guide/safari/manage-cookies-and-Services-data-sfri11471/mac (Safari); and
- https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy (Edge).

Navigation

When accessing and/or using the Services, non-identifying data may be collected, which may include the IP address, geolocation, a record of how services and Services are used, browsing habits and other data that cannot be used to identify the User.

The Services use the following third-party analysis services: Google Analytics

The Company uses the information obtained to obtain statistical data, analyze trends, administer the Services, study navigation patterns and to gather demographic information.

Accuracy and veracity of Personal Data

You agree that the information provided to the Company is correct, complete, accurate and current. You are solely responsible for the veracity and correctness of the data you submit

when access and/or using the Services, exonerating the Company from any responsibility in this regard.

Acceptance and consent

You declare to have been informed of the conditions on protection of Personal Data, You accept and consent to the treatment of the same by the Company in the manner and for the purposes indicated in this Privacy Policy.

Contact Data Protection Officer

For any questions or requests regarding this Privacy Policy, or to exercise the rights of access, rectification, cancellation, portability and opposition, you must contact our Data Protection Officer at:

Name: Alex Jones
Email: info@parityusd.fi
Address: Euro House, Richmond Hill Road, Kingstown, St Vincent and the Grenadines

When writing to our Data Protection Officer, please indicate:

1. a description of your query or request with the relevant details; and
2. the nature of your query or request in the subject header (for example, Correction of Personal Data Request, or Personal Data Access Request).

Change of Operatorship

In case of incorporation, acquisition, merger or any other causes that cause the change of Operatorship of the Services, you expressly consent that your registration data and information are transferred by the Company to the new Operator. When and if this occurs, the Company will comply, in any case, with the duty of information to you.

Amendment to this Privacy Policy

We continually improve our methods of communication and add new functionality and features to our platforms and services. As such, we keep our Privacy Policy under review and we may amend it. We reserve the right to make changes and updates to this Privacy Policy without giving you prior notice. We encourage you to check this Privacy Policy frequently and anytime you submit personal data via our platform. You are responsible for keeping track of the changes made to the Privacy Policy. Your continued use of the Services shall constitute your agreement to be bound by any such changes to this Privacy Policy. If we make any changes, the updated Privacy Policy will be posted on the Website with a revised effective date.

Notice to California and Virginia Residents

Our Services are currently designed for use only outside of the United States. You should not use our Services from the United States.

However, in the case we collect Personal Data from California and Virginia residents, this section provides additional details about the Personal Data we might collect about California and Virginia residents and the rights afforded to them under the California Consumer Privacy Act ("**CCPA**") and the Virginia Consumer Data Protection Act ("**VCDPA**").

Subject to certain limitations and exceptions, the CCPA and VCDPA provide California and Virginia residents, respectively, with certain rights. Depending on the state in which you are a resident, you may have the right to:

- Confirm whether the Company processes your Personal Data;
- Correct inaccurate Personal Data;
- Request details (in a readily usable format) about the categories and specific elements of Personal Data we collect;
- Delete your Personal Data;
- Opt out of any sales, sharing, targeted advertising, or profiling for certain decisions (as these terms are defined in the CCPA and/or VCDPA); and
- Not be discriminated against for exercising these rights.

We do not sell information about you to third parties. In order to help the Company deliver advertising and marketing on other platforms, we do allow third parties to collect information through our Services. Please see the "Content from other Services" section above for more details.

We collect the following categories of personal information: identifiers (such as name, email address and IP address), Internet or other electronic network activity information (such as engagement with promotional messages and ads), and inferences (such as gender, based on your first name). For more details about the information we collect (including the categories of sources of this information) as well as the purposes for processing, please see the "What Personal Data we Collect" and "How we use your Personal Data" sections above. We share this information with the categories of third parties described in the "Disclosures of Personal Data" section above.

California and Virginia residents may make a request to exercise rights under the CCPA and VCDPA, respectively, that are not otherwise exempt under applicable law. You may also request assistance by sending an email to our Data Protection Officer. We may verify the request by asking you to provide information that matches information we have on file about you. You can also designate an authorized agent to exercise these rights on your behalf, but we will require proof that the person is authorized to act on your behalf and may also still ask you to verify your identity with us directly. If you are a Virginia resident and the Company is unable to satisfy your request to exercise a right available to you under the VCDPA, you are entitled to appeal our decision by emailing the Data Protection Officer.

Services Operator

The Services are operated by Horus Research LLC, a St Vincent and the Grenadines limited liability company registered under the Limited Liability Companies Act of St Vincent and the Grenadines and having its registered office at Euro House, Richmond Hill Road, Kingstown, St Vincent and the Grenadines.