Privacy Policy

1. Introduction

1.1. This Privacy Policy explains how Vertamon Sp. zo. o uses client's Personal Data (defined below) company provides access and utility through our digital asset trading platform via software, API (application program interface), technologies, products and/or functionalities ("Service"). In the course of providing Service, to abide by the laws in the jurisdictions that the company operates, and to improve services, company needs to collect and maintain personal information about the client. As a rule, the company never discloses any personal information about our customers to any non-affiliated third parties, except as described below.

1.2. Company may update this Privacy Policy at any time by posting the amended version on this site including the effective date of the amended version.

1.3. Company communicates any material changes to this Privacy Policy via email.

2. Definitions

2.1. Virtual Financial Asset

As used herein, "Virtual Financial Asset", also called "convertible virtual currency," "cryptocurrency," or "digital goods", such as bitcoin or ether, which is based on the cryptographic protocol of a computer network that may be

(i) Centralized or decentralized,

(ii) Closed or open-source, and:

(iii) Used as a medium of exchange and/or store of value.

2.2 Personal Data

As used herein, "Personal Data" means any information relating to an identified or identifiable natural person, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, economic, cultural or social identity of you as a natural person.

3. Collection of Personal Data

3.1. Company collects, processes, and stores Personal Data collected from you via client's use of the Service or where client has given consent.

3.2. This Personal Data may include contact details, copies of identification documentation provided by client or derived from publicly accessible databases, government identification number as well as information relating to devices or internet service (such as an IP address and a MAC number).Company collects information provided during the onboarding process, which may be a completed, incomplete, or abandoned process.

3.3. Company collects, uses, stores, and transfers Personal Data, which may include the following:

(i) Operating within the European Economic Area ("EEA").

(ii) Company collects, stores, and processes personal information in accordance with the Best Practices of Data Collection in the EU, in addition to GDPR [General Data Protection Regulation-(EU) REGULATION 679/2016].

(iii) Types of client defined in APPENDIX A.

4. Collection and Storing of Data Outside the EU

4.1. As outlined above, company may collect Personal Data from customers located in the EEA. To facilitate the services company provides to customers located in the EEA, company requests explicit consent for the transfer of Personal Data from the EEA to outside of the area. If client is an individual located in the EEA and declines to consent to such transfer, client will no longer be able to use company services.

4.2. Client will have the ability to withdraw digital assets; however, all other functionalities will be disabled.

5. Personal Data Usage

5.1. Company uses Personal Data to communicate with the client and to administer, deliver, improve, and personalize the Service. Company might also generate generic data out of any Personal Data collected and use it for company purposes.

5.2. Company may also use such data to communicate with you in relation to other products or services offered by company and/or its partners. Company does not share Personal Data with third parties (other than partners in connection with their services) except where client have given consent and further detailed below.

6. Company may share Client Personal Data with third parties:

6.1. If company deems that sharing it is necessary to enforce the Terms of Service ;

6.2. To comply with government agencies, including regulators, law enforcement and/or justice departments ;

6.3. To third parties who provide services to the company (such as administration or technical service;

6.4. in connection with the sale or transfer of our business or any part thereof.

6.5. Additionally, company has implemented international standards to prevent money laundering, terrorist financing and circumventing trade and economic sanctions and will implement final Virtual Financial Asset rules and regulations when effective, which will likely require us to undertake due diligence on our customers.

6.6. This may include the use of third-party data and service providers which we will cross-reference with your personal information.

7. Storage of Personal Data

7.1. The data that company collects from the client may be transferred to, and stored at, a destination outside of the EU.

7.2. It may also be processed by staff operating outside of the EU who work for the company or for one of company suppliers. By submitting client personal data, client agrees to this transfer, storing or processing, except customers located in the EEA, as detailed above.

7.3. All information you provide to us is stored on company and/or third party cloud servers.

8. Access and Correction of Personal Data

8.1. Client has the right to obtain a copy of Personal Data upon request and ascertain whether the information company holds about client is accurate and up-to-date.

8.2. If any of the Personal Data is inaccurate, client may request to update the information. Client may also request to delete Personal Data, with exception that the company may refuse client deletion request in certain circumstances, such as compliance with law or legal purposes. For data access, correction, or deletion requests, please contact company.

8.3. In response to data access, correction, or deletion request, company will verify the requesting party's identity to ensure that he or she is legally entitled to make such request. While company

aims to respond to these requests free of charge, company reserve the right to charge client a reasonable fee should the request be repetitive or onerous.

9. Marketing

9.1. Company may communicate company news, promotions, and information relating to our products and services provided. Company may share Personal Data with third parties to help with marketing and promotional projects, or sending marketing communications. By using our services, client accepts this Privacy Policy and agrees to receive such marketing communications.

9.2. Customers can opt out from these marketing communications at any moment. If you do not want to receive these communications, please send an email to support@palaris.io or conact +48-221-047-639

9.3. For product related communications, such as policy/terms updates and operational notifications, client will not be able to opt out of receiving such information.

10. Information Security

Company endeavors to protect clients from unauthorized access, alteration, disclosure, or destruction of Personal Data that the company collects and stores. Company take various measures to ensure information security, including encryption of the communications with SSL; required two-factor authentication for all sessions; periodic review of our Personal Data collection, storage, and processing practices; and restricted access to client's Personal Data on a need-to-know bases for our employees and vendors who are subject to strict contractual confidentiality obligations.

11. Contacting Company about Privacy Concerns

If client has any questions about this Privacy Policy or the use of Personal Data, please contact the company by sending an email to the following address support@palaris.io with the subject "PRIVACY REQUEST" or conact +48-221-047-639

12. Changes to Privacy Policy

Any changes made to company Privacy Policy in the future will be posted on this company website and, when appropriate, company will notify client by email.

APPENDIX A

Definition of Clients

1. Individual clients:

Email address

Mobile phone number

Full legal name (including former name, and names in local language)

Nationality

Passport number, or any government issued ID number

Date of birth ("DOB")

Proof of identity (e.g. passport, driver's license, or government-issued ID)

Residential address

Proof of residency

Additional Personal Data or documentation at the discretion of our Compliance Team

2. Corporate clients:

Corporate legal name (including the legal name in local language)

Incorporation/registration Information

Full legal name of all beneficial owners, directors, and legal representatives

Address (principal place of business and/or other physical locations)

Proof of legal existence

Description of the business

Percentage of ownership for Individual/corporate owners

Contact information of owners, principals, and executive management (as applicable)

Proof of identity (e.g., passport, driver's license, or government-issued ID) for significant individual beneficial owner of the institutional customer entity

Personal Data for each entity's significant beneficial owner of the institutional customer entity (see the "Individual Customer" section above for details on what Personal Data we collect for individuals)

Source of wealth

Amount of bitcoin or other digital assets projected to be injected