

## **CRYPTICS PRIVACY POLICY**

This privacy policy has been compiled to better serve those who are concerned with how their personal data is being used by CrypticsTech OÜ an Estonian company with the address at Harju maakond, Tallinn, Kesklinna linnaosa, Narva mnt 4, 10117, Estonia (hereafter “Controller”).

Please read our privacy policy carefully to get a clear understanding of how we collect, use, protect or otherwise handle your personal data.

As data controller, we determine the means and purposes of processing data in relation to the sale of our tokens. If you have any questions about your personal information or this privacy policy, please direct your questions to support@cryptics.tech.

### **PERSONAL DATA COLLECTED**

Personal data is data that can be used to identify you directly or indirectly. Our privacy policy covers all personal data that you voluntarily submit to us and that we obtain from our partners. This privacy policy does not apply to anonymised data as this cannot be used to identify you.

We may collect the following types of information:

- **Personal Identification Information:** Full name, date of birth, age, nationality, gender, signature, utility bills, photographs, phone number, home address, and/or email.
- **Formal Identification Information:** Tax/ other ID number, passport number, driver’s license details, national identity card details, photograph identification cards, and/or visa information.
- **Financial Information:** Bank account information, payment card primary account number (PAN), transaction history, trading data, and/or tax identification.
- **Transaction Information:** Information about the transactions you make on our services, such as the name of the recipient, your name, the amount, and/or timestamp.
- **Employment Information:** Office location, job title, and/or description of role.
- **Online Identifiers:** Geo location/tracking details, browser fingerprint, OS, browser name and version, and/or personal IP addresses.
- **Usage Data:** Survey responses, information provided to our support team, public social networking posts, authentication data, security questions, user ID, click-stream data and other data collected via cookies and similar technologies.

### **HOW YOUR PERSONAL INFORMATION IS USED**

We collect personal data to provide you with our services. When we require certain personal information from users it is because it is necessary for the specified purposes. Our primary purpose in collecting personal information is to provide you with a secure, smooth, efficient, and customised experience. In general, we use

personal data to create, develop, operate, deliver, and improve our services, content and advertising, and for loss prevention and anti-fraud purposes. We may use this information in the following ways:

### **To maintain KYC-principles**

Sale of our tokens may infer the necessity for us to collect and use your personal identification information, formal identification information, financial information, transaction information, employment information, online identifiers, and/or usage data in certain ways. In addition, we may use third parties to verify your identity by comparing the personal information you provided against third-party databases and public records.

### **To provide Controller's services and sale of our tokens**

We process your personal data in order to provide the services to you, including to provide service information, customer services and quality control. For example, when you want to buy our tokens, we require certain information such as your identification and contact information. We cannot sale you the tokens without such information.

When selling the tokens Controller handles sensitive information, such as your identification and sometimes financial data – it is therefore very important for us and our investors that we are actively monitoring, investigating, preventing and mitigating any potentially prohibited or illegal activities, enforcing our agreements with third parties, and/or violations of our posted user agreement or agreement for other services. In addition, we may need to collect fees based on your use of our services. We collect information about your account usage and closely monitor your interactions with our services. We may use any of your personal data collected on our services for these purposes.

### **For research and development purposes**

We process your personal data to better understand the way you use and interact with Controller. In addition, we use such information to customise, measure, and improve Controller's services and the content and layout of our website and applications, and to develop new services. Without such processing, we cannot ensure your continued enjoyment of our services. Our basis for such processing is based on legitimate interest.

We process this personal information to pursue our legitimate interests as described above.

We will not use your personal data for any other purposes than those described in this policy, without informing you. From time to time we may request your permission to allow us to share your personal data with third parties. You may opt out of having your personal data shared with third parties. If you choose to so limit the use of your personal data, certain features or Controller's services may not be available to you.

## **PERSONAL DATA FROM THIRD PARTY PROVIDERS**

Controller primarily collects personal data about you from you. From time to time, we may, however, also collect data about you from third party sources, such as public databases, credit bureaus, ID verification partners, resellers and channel partners, joint marketing partners, and social media platforms.

We obtain information about you from public databases and ID verification partners for purposes of verifying your identity. ID verification partners use a combination of government records and publicly available information about you to verify your identity. Such information includes your name, address, job role, public employment profile, credit history, status on any sanctions lists maintained by public authorities, and other relevant data.

## **COLLECTION AND USE OF INFORMATION COLLECTED AUTOMATICALLY**

We may receive and store certain types of information automatically, such as whenever you interact with the our website. This information does not necessarily reveal your identity directly but may include information about the specific device you are using, such as the hardware model, device ID, operating system version, web-browser software (such as Firefox, Safari, or Internet Explorer) and your Internet Protocol (IP) address/MAC address/device identifier.

For example, we may automatically receive and record information on our server logs from your browser, including your IP address; device type and unique device identification numbers, device event information (such as crashes, system activity and hardware settings, browser type, browser language, the date and time of your request and referral URL), broad geographic location (e.g. country or city-level location) and other technical data collected through cookies, pixel tags and other similar technologies that uniquely identify your browser. We may also collect information about how your device has interacted with our website, including pages accessed and links clicked. We may use identifiers to recognise you when you arrive at the Site via an external link, such as a link appearing on a third party site.

### **Cookies**

One method Controller may use to collect data about your use of Controller's services is through the use of cookies (small files placed on your hard drive). These help to analyze visits to our services and help us to deliver a more useful final product. You can manage cookies through the settings of your internet browser. You can have the browser notify you when you receive a new cookie, delete individual cookies or delete all cookies.

## **OUR SHARING OF PERSONAL DATA WITH OTHER PARTIES**

We take care to allow your personal data to be accessed only by those persons at Controller who really need to – and only when it is necessary – in order for them to perform their tasks and duties. Furthermore, we only share your data with third parties who have a legitimate purpose for accessing it and with the appropriate legal basis. **Controller will never sell or rent out your personal information.** We will only share your information in the following circumstances:

- We share your information with financial institutions with which we partner to process payments.
- We may share your information with law enforcement, officials, or other third parties when we are compelled to do so by a subpoena, court order, or similar legal procedure, or when we believe in good faith that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity or to investigate violations of our user agreement or any other applicable policies.

## **HOW WE PROTECT AND STORE PERSONAL INFORMATION**

We understand how important your privacy is, which is why Controller maintains (and requires its service providers to maintain) appropriate physical, technical and administrative safeguards to protect the security and confidentiality of the personal information you entrust to us.

We may store and process all or part of your personal and transactional information, including certain payment information, such as your encrypted bank account and/or routing numbers, in the United States and elsewhere in the world where our facilities or our service providers are located. We protect your personal information by maintaining physical, electronic, and procedural safeguards in compliance with the applicable laws and regulations.

## **YOUR RIGHTS**

When we process your personal data, you have a number of rights under the General Data Protection Regulation.

In general, you have a right of access to Controller's processing of your data. This means that you can ask us for information about our processing of your data and for a copy of the data. You also have the right to have a copy of your personal data transmitted to another enterprise, where technically feasible.

In addition, you have a right to object to our processing of your data. If the situation should occur, we will decide whether we are able to meet your objection. If that is the case, we will no longer process the data in question.

Finally, you have a right to have erased, blocked or rectified any data that turn out to be inaccurate or misleading or in a similar way have been processed in conflict with legislation.

## **COMPLAINTS**

Complaints about our processing of your personal data, can be filed at The Estonian Data Protection Agency.

## **CONTACT AND NEWSLETTERS**

If you have given your consent, Controller may contact you via the address, e-mail and / or phone number you provide on your account for marketing, surveys, news and/or similar initiatives.

## **ENCRYPTION OF DATA TRAFFIC**

Controller is committed to handling your Customer Information with the highest standards of information security. When your information is transferred over the internet, SSL encryption is used to ensure your sensitive data is not accessible to anyone on the internet. The data that is communicated back and forth between Controller and your computer is encrypted with a 256-bit SSL certificate. This means no one can intercept the data stream between Controller and your device.

## **GOVERNING LAWS**

Information collected through Controller will be treated in accordance with current Estonian legislation and the EEA Data Protection Law.