Charism Network Interface Privacy Policy

Last updated on September 1, 2022

Welcome to Charism's privacy policy (**“Policy”**).

The Charism network interface is maintained by Charism LLC. It is located at: Suite 336, Beachmont Business Centre, Kingstown, St. Vincent and the Grenadines, registration code 1999 LLC 2022. It controls your Personal Data under this Privacy Policy. This Privacy Policy explains how and why we may collect, store, use and/or transfer (“process”) your information while using our service (“Service”).

Therefore, the purpose of this Policy is the basis for the processing of your Personal data when you:

1. visit and use the Choose.com website, regardless of where you visit or use it;
2. apply for and register a customer account with us (your **“Account”**);
3. apply for and/or use any of our Services.

This also includes any data you may provide to us for our events, as well as other materials.

If you do not have the rights to act on behalf of a company or other organization, do not open or use the interface.

To better understand our practices regarding your Personal data, please read the following information carefully:

1. Changes to this Agreement.

We may update this privacy notice. The updated version will be marked with the “Revised” date. It will take effect as soon as it becomes available. If we change the privacy notice, we will inform you by posting a notice of such changes in a conspicuous place or by sending you notifications directly. To be aware of how we are protecting your information, you should review this privacy notice.

2. Eligibility.

Age. By using the Service, you represent that you are at least eighteen (18) years of age. If you are under eighteen (18) years of age, you may not use the Interface. If we learn that a user is under the age of eighteen (18), we will deactivate the account and delete the data from our records. Please also let us know if you become aware of any data from children under eighteen (18) years of age.

3.Applicability.

This Privacy Policy applies to all of your interactions with us through the Service and your interactions with us. Below are the categories of our processors used on the Website in connection with the internal data processing roadmap. This gives an overview of our data processing activities. This is where the personal information we may collect through the Interface resides. The following are the categories of our processors who may access and process your Personal data through the Interface:

1) Maintenance providers;
2) Project and team management providers;

3) Suppliers of merch products;
4) Communication providers;
5) Analytics, statistics, performance, marketing vendors.

4. Data processing.

Data we collect about you:

Personal data or personal information means any information about an individual to identify him. This does not include anonymous data (**anonymous data**).

We may collect and use different types of Personal data about you that we have aggregated (**for purely indicative purposes**). For the avoidance of doubt, categories marked in blue do not apply to non-customers (persons who do not have a registered account).

- **Identity data** includes your first name, maiden name (if applicable), last name, username or similar identifier, marital status, title, nationality, date of birth, gender, ID and/or passport number.
- **Contact information** includes address, billing address, email address and contact number.
- **AML and KYC data** includes the following due diligence documentation and information about you:

(i) a copy of your identity document, passport and/or driver's license, (ii) proof of residence (such as a recently issued utility bill), (iii) “selfie” (for identity verification), (iv) verification KYC databases, (v) fraud database checks, and (vi) any documentation or information you may need:

- to ensure compliance with legislation and global AML/KYC practices; and/or

- to any competent authority authorized to collect information, including any other documentation or information that is prescribed by applicable law and any other competent authority (including foreign authorities and foreign laws in force).

- Enhanced KYC data applies to payments that exceed a set threshold. They include, at the very least, documentation and information about the due diligence of the client and their source of funds.
- Financial data includes wallet and private key information.
- Transaction data includes information about:

    o your subscriptions, purchases and transactional activity;
    o the history of your transactions on the Platform;
    o your use of the Services;
    o payments you made.

- **Portfolio data** includes information about the tokens that are credited to your account.
- **Usage data** includes information about how you use our Platform and the Websites.
- **Technical data** includes internet protocol (IP) address, login information, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technologies on the devices you can use to access and view websites.
- **Website Visit data** includes resource locators (URLs), the sequence of visits to the website, including date and time, and the products you viewed or searched for, page response time,

download errors, duration of visits to certain pages, information about interaction with the page, and the methods used to navigate away from the page.
- **Marketing and communications data** tells you about your preferences regarding marketing materials from us, as well as your communications preferences. This may include information about subscribing, attending our events, or accepting our invitations.

However, we will not ask you to share your private keys or wallet seed. Do not trust anyone or any website that asks you to enter your private keys or wallet seed.

How and Why we use your Personal Data

We will only use your Personal data as permitted by law. Most often, we will use your Personal data in the following cases:

- If you want to enter into a client relationship with us.
- When entering into a contract (including in relation to your purchases of tokens and subscriptions, and use of the Services).
- To serve our interests (or the interests of a third party) and your interests and fundamental rights do not override those interests.
- When we need to comply with legal or regulatory obligations.

We may use the personal data described above or any other Personal data:

- Based on the performance of a contract or the need to enter into a contract (when we need the Personal data to fulfill our obligations and obligations under the contract, and when you use our services, or when we are in the negotiation phase);
- For the purposes of our interests or the legitimate interests of our processors to protect the Interface, to prevent any malicious activity on the Interface, to maintain the security of our technical systems, to improve services and products using statistics;
- To respond to legal requests from authorities, provide information on court orders and decisions, or where we have a good faith belief that such disclosure is necessary and to comply with the law to comply with official investigations or legal proceedings initiated by government and/or law enforcement officials, or individuals, including but not limited to: in response to a subpoena, search warrant or court order, and without limitation other similar statutory obligations;
- Based on your consent; as well as
- On other legal grounds provided for by the legislation on the protection of personal data.

Disclosure of your Personal data

We may need to access your Personal data for the parties listed below for the purposes (see table in **Clause 5** above) for:

- **Third party service providers**, including platform integration and infrastructure hosting service providers (for data storage), KYC service providers and customer identification and verification service providers (for ease of setup), payment services and payment gateways (for payment processing), and also token accounting services (to verify, monitor and protect token subscriptions, purchases, as well as trading activities).
- **Our affiliates**, such as partner firms involved in providing certain Services.
- **Affiliated groups of companies**. We share information with these organizations to:

a) assist, detect and prevent potentially illegal activities and violations of our policies;

b) allow you to use the Company's products and services; as well as

c) guide decisions about our products, services and communications.

- **Suppliers and external agencies** that we engage to process and provide information and/or materials that you may have requested.
- **Professional consultants** (consultants, bankers, professional insurers, brokers and auditors).
- **Law enforcement, public authorities and judiciary** (local and foreign).
- **Other organizations** where information is shared for fraud protection or credit risk mitigation purposes.
- **Debt collection agencies** that help us collect debts.
- Third parties to whom we may sell, transfer or combine parts of our business or our assets (**successors in title**). We may also acquire or merge with other businesses. If our business changes, the new owners may use your Personal data in the same way as described in this Policy.

We require all affiliates and third party service providers to respect the security of your Personal data. They must treat them in accordance with the law. We do not allow them to use your Personal data for their own purposes. The processing of your Personal data should only take place for specific purposes and in accordance with our instructions. Our service providers currently store your Personal data in Germany. We will update this Privacy Policy if the location where their data is stored changes.

Data Retention Period

We treat our relationship with customers as permanent until terminated by us or the customer in accordance with our Terms of Use.

We will retain your Personal data for as long as it is necessary to achieve the objectives of our policy, **namely:**

- to comply with any legal, accounting, tax, anti-corruption, regulatory or reporting obligations to which we may be subject (including as an issuer of a virtual financial asset under applicable Estonian law); and/or
- to the extent that we may also need to retain your Personal data in order to be able to bring or defend possible future legal claims against you or otherwise related to you.

In general, we will not retain your Personal data for more than **six (6) years** from the date you terminated your customer relationship with us. As a rule, this usually occurs as a result of the closure or termination of your client account. This allows us to use your Personal data to fulfill any AML/CFT retention and reporting obligations and to filing, exercising or defending against possible future legal claims (subject to the statute of limitations). In some cases, we may need to retain your Personal data for up to **ten (10) years** to comply with accounting and tax laws (primarily for Transaction data). There may also be cases where it is necessary to store Personal data for longer periods due to the nature of the products and services provided.

In some cases, you may ask us to delete your data.

5. Cookies and Automatically Collected data.

When you use our Website, we may ask you to consent to the use of cookies. They are small files placed on the hard drive/browser of your computer or mobile device and web beacons (small electronic files) that are located on the pages of the Interface to collect certain information about the devices you use and your online activities.

The data automatically collected from cookies and web beacons may include information about your web browser and information about your visits to the Interface (traffic, location, logs, page views, visit duration, website navigation paths), as well as information about your device and Internet connection, including your IP address and how you interact with the Interface. We collect this data to help us improve the Interface and the user experience.

The information we collect automatically may also include statistics and performance information during your use of the Interface. This data type will be used by us only in aggregated form.

You can set your browser to refuse all or some browser cookies or notify you when the Website sets or accesses cookies. If you disable or refuse cookies, please note that some parts of the Website may become inaccessible or not function properly.

6. Your rights under the GDPR.

Under certain circumstances, you may have a number of privacy rights in relation to the use, storage and processing of your Personal data (for example, the right to have your data deleted).

You have the right:

1. **Request access** to your Personal data. In this way, you can obtain a copy of the Personal data and check whether we are processing it lawfully.

2. **Obtain information** when collecting and processing Personal data about you from publicly available or third-party sources. When this happens, we will notify you as soon as reasonably practicable of the third party or public source from which we obtained your Personal data.

3. **Request correction or rectification** of the Personal data we hold about you. This allows you to correct and/or update any inaccurate data we hold about you. In doing so, we may need to verify the accuracy of the new data you provide to us. As mentioned, it is in your best interest to keep us informed of any changes or updates to your Personal data that may occur.

4. **Request erasure** of your Personal data. This allows you to ask us to remove or remove Personal data if:

    - we have no good reason to continue processing them;
    - you have successfully exercised your right to object to processing (see below);
    - we may have processed your information unlawfully; or
    - we are required to delete your Personal data in accordance with local law.

However, we may not always be able to comply with your deletion request for legal reasons, of which you will be notified. This may include cases where the retention of your Personal data is necessary for:

- comply with legal or regulatory obligations to which we are subject; or
- execution of a lawsuit.

5. **Object to processing** of your Personal data where we are relying on a legitimate interest (or the interest of a third party). However, there is something about your situation that makes you object to processing on this basis because you consider that it affects your fundamental rights and freedoms. You also have the right to object when we process your Personal Data for direct marketing purposes.

In some cases, we may establish that we have compelling and legitimate grounds for processing your personal information that override your rights and freedoms.

6. **Request restriction of processing** of your Personal data. This allows you to ask us to suspend the processing of your Personal data in the following cases:

- if you want us to ascertain the accuracy of the data;
- when we use data illegally, but you do not want us to delete it;
- when you need us to keep the data, even if we no longer need it because you need it to establish, exercise or defend legal claims; or
- when you object to our use of your Personal data, but we need to verify that we have overriding legal grounds for using it.

7. **Request the transfer (data portability)** of your Personal Data to you or a third party. In this case, we will provide your Personal data in a structured format. Please note that this right only applies to automated information that you initially consented to using or where we used that information to perform a contract with you.

8. **Withdraw your consent at any time** of your Personal data. However, this will **not** affect the lawfulness of any processing we performed before you withdrew your consent. Any processing actions that are not based on your consent will remain in effect.

7. Transfer of Personal data.

We do not generally transfer your Personal data to third countries, except as necessary to: (i) process your transactions, subscriptions, purchases and/or trading activities, (ii) provide the services you have requested, (iii) perform our contractual obligations, (iv) compliance with our contractual rights and terms of service, (v) compliance with our obligations, or (vi) legal action.

Where we need to transfer your Personal data to third countries, we will provide the same degree of protection for that Personal data by providing at least one of the following security measures:

- We will only transfer your Personal data to countries that, in the opinion of the European Commission, provide an adequate level of protection for Personal data.
- In the absence of an adequacy decision, we will use special contracts approved by the European Commission that provide the same protection for Personal data as in Europe.
- When we use US providers, we may transfer data to them if they participate in the Privacy Shield, which requires them to provide similar protection for Personal data between

Europe and the US.

8. Data security.

We have put in place appropriate security measures to prevent accidental loss, use or unauthorized access to, alteration or disclosure of your Personal data. We also periodically review and, where possible, improve these security measures.

We also restrict access to your Personal data strictly to those employees who have a professional “need to know”. They will only process your Personal data in accordance with our instructions and are bound by confidentiality. All of our employees and agents have received appropriate data protection training.

Please note that no electronic transmission, storage or processing of Personal data is completely secure. We cannot guarantee that the security measures we have in place to protect Personal data will never be compromised or fail. Therefore, while we strive to protect your privacy, we do not promise, and you should not expect, that your Personal data will always remain private or secure.

We have put in place a procedure to deal with any alleged breach of Personal data and will notify you and any regulatory authority of a breach where we are required by law to do so.

9. Complaints.

You have the right to lodge a complaint at any time with a competent data protection supervisory authority, for example the supervisory authority in your place of permanent residence or work.

However, we would appreciate the opportunity to resolve your concerns before you contact the supervisory authority, so please contact us first.