CHRONOS GLOBAL UAB
Eisiskiu sodu 18-oji st.11
Vilnius, Lithuania

PRIVACY POLICY

CryptoOrange (also referred to as "we", "us", or "our", "CHRONOS GLOBAL UAB") is a company registered in Vilnius, Lithuania (EU) (Company no. 305947127). Our registered address is Eisiskiu Sodu 18-oji st.11, Vilnius, Lithuania (EU).

The purpose of this policy

This Policy is designed to help you understand what kind of personal data we collect in connection with our services and how we will process and use this information. When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control. This Policy describes how we collect, use, share, retain and safeguard personal data. This Policy also helps you to understand your legal rights to your personal data and explains our lawful basis for processing personal data and who to contact should you have a query on the collection and use of your personal data.

What is personal data?

Personal data is information relating to an identified or identifiable natural person. Examples include an individual's name, age, date of birth, gender, contact details, national identity number and passport details.

Personal data we collect

To allow us to provide you with our services we will collect and process personal data about you. We will collect this information when you register for our services, when you request information of our services, or when contacting us for technical assistance or for help navigating our website.

We will collect personal data when you first visit our website, where with your permission we will place a small text file which is commonly known as a cookie on your computer. Cookies are used to help identify visitors, to simplify accessibility when accessing the website and to monitor visitor's behaviour when viewing website content, navigating our website and when using website features.

We will also collect your unique online electronic identifier when visiting our website or application; this is commonly known as an IP address. Collecting IP addresses allows us to calculate the number of website visitors and to help identify the origin of any malicious actions that are performed against our website.

The personal data we will collect includes the following categories of personal data:

- Personal data such as an individual's name, address, date of birth, gender, contact and passport details, IP address, and details relating to national insurance or national identity number; and
- Data relating to criminal convictions and offences such as details on fraud and money laundering.

CHRONOS GLOBAL UAB
Eisiskiu sodu 18-oji st.11
Vilnius, Lithuania

Why do we need your personal data?

Your personal data is required to enable us to provide you with our services, to verify your identity and to perform anti money laundering screening, to respond to any requests from you about services we provide and to process complaints.

Data we share

We do not share your personal information with companies, organizations, or individuals. However, we will share your personal data with authorized third parties. This is necessary where we are required to do so by law. Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request.

If you object to the collection, sharing and use of your personal data we may be unable to provide you with our services.

Our lawful basis for processing your data

When registering for our products and services you should understand that you are forming a contract with us. When you request details on the services we provide, if you allow us to market to you, we would consider ourselves as having a legitimate business interest to provide you with information on similar services we provide. 'Performance of a contract' and 'legitimate interest' form our lawful basis for processing your personal data and for marketing to you. We will also ask for your consent in order to carry out AML/KYC Checks, when signing up.

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published. Please visit our platform regularly in order for checking whether Privacy Policy changed.

Retaining your data

We will retain your personal data when registering for our services for a period of you holding account at our website and after closing. Some of the data as specified in our AML Guidelines shall be entered in the logbook (as described in the AML Guidelines) in chronological order on the basis of documents confirming a Monetary Operation or transaction or other legally valid documents related to the execution of Monetary Operations or transactions, immediately, but not later than within 3 business days after the execution of a Monetary Operation or transaction.

The data specified above shall be retained for 8 years after the expiry of the Business Relationship or the completion transaction. The data related to the performance of the reporting obligation must be retained for 5 years after the performance of the reporting obligation. The correspondence of a Business Relationship with the Customer must be retained for 5 years from the date of termination of transactions or Business Relationship.

Documents and data must be retained in a manner that allows for exhaustive and immediate response to the queries made by the FCIS or, pursuant to legislation, other supervisory authorities, investigation authorities or the court.

The Company implements all rules of protection of personal data upon application of the requirements arising from the applicable law. The Company is allowed to process personal data gathered upon CDD implementation only for the purpose of preventing Money Laundering and Terrorist Financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

The Company deletes the retained data after the expiry of the time period, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a precept of the competent supervisory authority, data of importance for prevention, detection or investigation of Money Laundering or Terrorist Financing may be retained for a longer period, but not for more than two years after the expiry of the first time period. Where you or law enforcement agencies inform us on any active investigation or potential criminal prosecution, we will comply with all legal requirements for retaining this data.

The retaining of data is necessary for business administration and legal purposes. Sometimes we may need to retain your data for longer, for example if we are representing you or defending ourselves in a legal dispute or as required by law or where evidence exists that a future complaint may occur.

Your rights

Individuals are provided with legal rights governing the use of their personal data. These grant individuals the right to understand what personal data relating to them is held, for what purpose, how it is collected and used, with whom it is shared, where it is located, to object to its processing, to have the data corrected if inaccurate, to take copies of the data and to place restrictions on its processing. Individuals can also request the deletion of their personal data.

These rights are known as Access Rights. The following list details these rights:

- The right to be informed about the personal data being processed;
- The right of access to your personal data;
- The right to object to the processing of your personal data;
- The right to restrict the processing of your personal data;
- The right to rectification of your personal data;
- The right to erasure of your personal data;
- The right to data portability (to receive an electronic copy of your personal data);
- Rights relating to automated decision making including profiling.

Individuals can exercise their Access Rights at any time. We will not charge a fee to process these requests, however if your request is considered to be repetitive, wholly unfounded and/or excessive, we are entitled to charge a reasonable administration fee or to refuse your request.

In exercising your Access Rights, you should understand that in some situations we may unable to fully meet your request, for example if you make a request for us to delete all of your personal data, we may be required to retain some data for business administration or for prevention of crime purposes.

Protecting your data

We will take all appropriate technical, physical and organizational steps to protect the confidentiality, integrity, availability and authenticity of your data, including when sharing your data third parties. We will implement appropriate technical and organizational measures against unauthorized or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of personal data, and against accidental or unlawful loss destruction, alteration, disclosure or damage of personal data.

We build security into our services to protect your information. All our products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

We work hard to protect you us from unauthorized access, alteration, disclosure, or destruction of information we hold.

We also comply with certain legal frameworks relating to the transfer of data, such as the EU-US. When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

The Client is absolutely responsible for providing the confidentiality of passwords, user names other information about access to Personal account and Platform.

The Client is absolutely responsible for performed actions and operations with the usage of registration information. In the case of undesirable disclosure of information about personal login or password, the Client may change the password independently at the site of the Company. If personal information is disclosed (login or password) to the third parties due the fault of the Client, the Company is not responsible for information security and safety.

The Company guarantees the confidentiality of Clients and their private information and assumes all possible measures for its providing, including observation of standards of security during transmission of the confidential information and usage of present-day keeping technologies.

CHRONOS GLOBAL UAB
Eisiskiu sodu 18-oji st.11
Vilnius, Lithuania

Data privacy representative

To ensure data privacy and protection has appropriate focus within our organization we have appointed a Data Privacy Representative who reports into our senior management team. The contact details can be found at the end of this Privacy Policy.

Complaints

If you are dissatisfied with any aspect on how we process your personal data please contact our Data Privacy Representative. You also have the right to complain to the

How to contact us

If you have any questions regarding this Policy and its content, the use of your data and your Access Rights please contact our Data Privacy Representative at CryptoOrange address or by emailing info@cryptoorange.com.