

PRIVACY POLICY

This Privacy Policy (this “**Policy**”) applies to the trading platform (including any applicable mobile applications used to access the same) (collectively the “**Platform**”) and when you use our website columis.com (the “**Website**”) provided by Chronos Global, UAB (also referred to as “we”, “us”, or “our”, “Company”), company registered address is Konstitucijos pr. 26, 08131 Vilnius, Lithuania, legal entity code 305947127.

It describes how the Company collects, uses, and discloses Personal Data that Company obtains from users (the “**User**”) of the Platform and any account by services provided through the Platform as well as other our collected Personal Data, and how we use and disclose that information.

1. The purpose of this Policy

- 1.1. This Policy supplements the other notices and is not intended to override them. Terms used within it shall have the meaning(s) given in the Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)), as applicable.
- 1.2. Policy describes how the Company collects, uses, and discloses Personal Data that we obtain from you using the Platform and any services provided through the Platform as well as other collected Personal Data, and how we use and disclose that information.
- 1.3. 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 are trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.
- 1.4. 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.

2. What is Personal Data?

- 2.1. 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.

3. The Personal Data we collect about you and how we collect It

- 3.1. We collect and process Personal Data about you directly from you when you contact us, register to use the Platform, or submit such information as a part of the Know-Your-Client (“**KYC**”), as well as automatically through your use of the Platform. We may also collect or receive Personal Data from third party service providers, state institutions or other persons that may have a legal ground to provide the Personal Data to us.

4. Personal Data we collect directly from you

- a) **Identification Information:** We may collect the following information when you register an Account: full name, email address, password, country of residence, date of birth. When your Account meets certain standard, we may collect additional information: name as in identity card/passport, identity card/passport number and photo, date of expiry, mailing address, residential address, proof of address, mobile telephone number. We also collect any other information relating to you which you have provided to us in any forms that you may have submitted to us, or in other forms of interaction with you.
- b) **Biometric Data:** includes scan of face geometry, which we use for your identification.
- c) **Financial Information,** such as Your bank account information, credit card information (including the card number, expiry date and CVC), tax identification number, cryptocurrency wallet address, transaction history and trading data.
- d) **Transaction Information:** may include transaction information as you use our services, including deposit snapshots, account balances, trade history, order activity and distribution history, bank account number, identification data of electronic money account, account statement;
- e) **Information collected in accordance with the requirements of the laws:** Results from Politically Exposed Persons (PEP) screening & sanction screening, any additional Personal Data required for proving Source of Funds (e. g. employment contract, certificate of inheritance, etc.), biometric checks, AML screening, address, ID document, video and e-mail verification, data on the management structure and business activity, etc.
- f) **Profile Information:** includes your account full name and password as a password hash (encrypted), username, preferences, feedback, and survey responses.
- g) **Employment and Screening Information:** includes your employment history, education background and income levels, data relating to criminal convictions and offences such as details on fraud and money laundering.
- h) **Communications with Us:** We may collect information you give us during any support and feedback communications via email, telephone, or when you contact us through contact forms on the Platform. We use this information to respond to your inquiries, provide support, facilitate transactions, and improve our Platform.
- i) **Usage Information:** We may collect information about your use of our Platform, including cookies, IP (internet protocol) address, computer and connection information, device type and unique device identification numbers (e. g. IMEI number, MAC address), bandwidth, mobile network information, mobile operating system and type of mobile browser, statistics on page views, and traffic to and from our websites, and other technical data collected through cookies and other similar technologies that uniquely identifies your browser.
- j) **Marketing and Communications Data** includes your consent and preferences in receiving direct marketing from us and our third parties and your communication preferences.

- 4.1. Please note that if you are acting as an authorized individual on behalf of a User and are providing Personal Data for such User, you are responsible for ensuring that you have all required permissions and consents to provide such Personal Data to us for use in connection with the Platform and that our use of such Personal Data you provide to the Platform does not violate any applicable law, rule, regulation or order.

5. Why do we need your Personal Data?

- 5.1. 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.

6. How is your Personal Data collected?

- 6.1. We use different methods to collect Personal Data from and about you including through:

a) Direct interactions

- 6.2. You may provide us with your Personal Data by filling in forms or by corresponding with us via our Website or by post, phone, email or otherwise. This includes Personal Data you provide when you:

1. apply to use our services;
2. create an account on our Platform;
3. log into the Users account in the Platform and / or make transactions;
4. give us some feedback or lodge a query.

b) Third parties or publicly available sources

- 6.3. We may receive Personal Data about you from various third parties and public sources as set out below:

1. Our partner who shares your Personal Data with us so that (a) you can use our services on their behalf; and (b) they can pay money to you (for example, your salary if you are their employee or payment for goods and/or services if you are their supplier);
2. analytics providers such as Google based outside the EU;
3. advertising networks such as Google based inside OR outside the EU; and
4. search information providers Google based inside OR outside the EU;
5. Electronic Identity Verification providers from data brokers or aggregators based inside or outside the EU;
6. We may also record and verify personal identity documents such as passports electronically including screen grabs;
7. Identity data and contact data from publicly available sources based inside the EU;

- 6.4. To provide contracted services, we may need verify details with Credit Reference agencies, anti-Fraud agencies, Sanction screening and politically exposed persons (PEP) listings.

7. Data we collect automatically

- 7.1. When you use the Platform, our servers automatically record information using cookies and other tracking technologies, including information that your browser sends whenever you visit the Platform or your mobile application sends when you are using it. This log data may include your Internet Protocol address, your browser type and settings, the date and time of your request, language preferences, and cookie data.
- 7.2. In addition to log data, we may also collect information about the device you use for the Platform, including what type of device it is, what operating system you are using, device settings, unique device identifiers, and crash data. Whether we collect some or all this information may depend on what type of device you are using and its settings.
- 7.3. We may combine this information with other information that we have collected about you, including, where applicable, your full name, username, email address, and other Personal Data.
- 7.4. **Geolocation.** If you have provided permission through your mobile device to allow us to collect location information through a mobile application, we may obtain your physical location information in terms of latitude and longitude from technologies like GPS, Wi-Fi, or cell tower proximity. You can withdraw your permission for us to acquire such physical location information from your mobile device through your mobile device settings, although we do not control this process. If you have questions about how to disable your mobile device's location services, we recommend you contact your mobile device service provider or the mobile device manufacturer.

8. Our lawful basis for processing your Personal Data

- 8.1. We process your Personal Data using one of the following legal basis:
- a) **Performance of a contract** means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering such a contract;
- b) **Legitimate interest** means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your Personal Data for our legitimate interests. We do not use your Personal Data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us;
- c) **Legal requirement** means processing your Personal Data where it is necessary for compliance with a legal or regulatory obligation that we are subject to;

d) Consent means processing your Personal Data using your written consent.

- 8.2. Note that we may process your Personal Data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground, we are relying on to process your Personal Data.
- 8.3. Generally, we do not rely on consent as a legal basis for processing your Personal Data other than in relation to sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

9. How we use your Personal Data

- 9.1. We will only use your Personal Data when the law allows us to. Most commonly, we will only disclose your Personal Data to the third parties which shall be considered as data processors for the following purposes:
- To provide our Platform to you, to facilitate communications and transactions on the Platform, to communicate with you about your use of our Platform, to respond to your inquiries, to fulfill your orders, and for other customer service purposes;
 - To process transactions – in order to allow you to make the payment(s) and/or receive funds through your payment devices and by the Platform;
 - To verify your identity - in order to verify your identity, perform transactions you instruct on us or for the purposes of fraud detection or protection, or in other situations involving suspicious or illegal activities we use and share your data with credit-checking/reference agencies and fraud prevention agencies. We may as well perform a search of your credit file, if this is necessary and/or required to deliver our services to you;
 - To perform our services and payments – we use and share your data with banking, including Electronic Money Institutions, crypto exchanges and financial service partners such as banking intermediaries, international payment services providers and regulated distribution agents;
 - To tailor the content and information that we may send or display to you, to offer location customization, and personalized help and instructions, and to otherwise personalize your experiences while using our Platform;
 - To better understand how Users access and use the Platform, both on an aggregated and individualized basis, in order to improve our Platform and respond to User desires and preferences, and for other research and analytical purposes;
 - To manage our relationship with you, including notifying you about changes to our Terms or Policy, ask you to leave a review or take a survey;
 - To enable you to partake in a prize draw, competition or complete a survey;

- To pursue legitimate interests of the Company – video or electronic surveillance for the protection of property and health, legal compliance, IT systems monitoring, fraud prevention, debt management;
- To administer and protect our business and this Website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data);
- For direct marketing and promotional purposes. For example, we may use your information, such as your email address, to send you news and newsletters, special offers, and promotions, to conduct sweepstakes and contests, or to otherwise contact you about products or information we think may interest you. We also may use the information that we learn about you to assist us in advertising our Platform on third-party websites.

9.2. In addition, we or our partners may transfer or disclose your Personal Data to:

- comply with any legal obligation required under legal requirement (e. g. to state authorities);
- enforce any part of our agreements concluded between you and us or to investigate potential breaches; or
- protect our rights or our property, or those of our other clients. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

9.3. We require all third parties to respect the security of your Personal Data and to treat it in accordance with the law. We do not allow our third-party service providers to use your Personal Data for their own purposes and only permit them to process your Personal Data for specified purposes and in accordance with our instructions.

10. How we share your Personal Data

10.1. **Affiliates.** We may disclose the Personal Data we collect from you to our affiliates or subsidiaries solely for the purpose of providing the Platform to you; however, if we do so, their use and disclosure of your personally identifiable information will be maintained by such affiliates and subsidiaries in accordance with this Policy.

10.2. **Service Providers.** We may disclose the information we collect from you to third-party vendors, service providers, contractors or agents who perform functions on our behalf (e.g. auditors, accountants, lawyers, credit-checking/reference agencies and fraud prevention agencies, banking institutions), provided such third parties have agreed to only use such information to provide services to us.

10.3. **Business Transfers.** If we are in negotiations with, or are acquired by or merged with another company or entity, if substantially all of our assets are transferred to another company or entity, or as part of a bankruptcy proceeding, we may transfer the information we have collected from you to the other company or entity.

10.4. **In Response to Legal Process.** We also may disclose the information we collect from you in order to comply with the law, a judicial proceeding, court order, or other legal process, such as in response to a subpoena.

- 10.5. **To Protect Us and Others.** We also may disclose the information we collect from you if we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of our Service Agreement or this Policy, or as evidence in litigation in which we are involved.
- 10.6. **Aggregate and De-Identified Data.** We may collect, process, analyse and share aggregate or de-identified information about Users with third parties and publicly for product development, marketing, advertising, research or similar purposes.

11. Our Use of Cookies

- 11.1. We and our third-party service providers use cookies and other tracking mechanisms to track information about your use of our Platform. We may combine this information with other Personal Data we collect from you (and our third-party service providers may do so on our behalf).

- 11.2. The following cookies are used by the Platform:

Cookie name	Description/Purpose	Moment of creation	Validity period/Expiry	Data used	Type
XSRF-TOKEN	This cookie is essential for security. It stores a CSRF (Cross-Site Request Forgery) token, which helps protect the application from malicious requests by verifying that any requests coming in are genuinely from the application and not a third-party attacker.	This cookie is typically created when a user initiates a session with the application (e.g., when they visit the site).	Session	It contains a unique, encrypted token generated by Laravel. This token is used to validate incoming requests.	HTTP Cookie
laravel_session	[_] This cookie is vital for session management. It stores the user's session data, allowing the application to maintain their state	Created upon the start of a user's session with the application.	Session	Contains encrypted session data, which may include user ID (if logged in), flash messages, and	HTTP cookie

	across different requests. This includes information like login status, session variables, and other session-related data.			any other data stored in the session.	
io	This cookie is associated with the Socket.IO library, which facilitates real-time communication between the application and the user's browser	Created when the user's browser establishes a Socket.IO connection with the application.	Session	Contains data related to the Socket.IO connection, such as session ID, connection ID, or other information required to manage the real-time communication channel.	HTTP cookie (Socket.IO connection management)

- 11.3. To manage cookies, you can adjust the browser settings. Disabling all the cookies can rise privacy level but it also can restrict use of some functions of the Website. You can find information about how to manage cookies in the most commonly used browsers at the following addresses: Google Chrome, Mozilla Firefox, Apple Safari, and Microsoft Internet Explorer.

12. Personal Data transfer

- 12.1. We may transfer your data outside of the EEA. Such transfers are carried out in compliance with the GDPR, for instance appropriate Standard Contractual Clauses and/or Adequacy decisions are set in place to ensure that your Personal Data is treated securely and in accordance with this Policy.
- 12.2. Would you like to receive more information (copy) of relevant safeguards, please reach out to us at info@columis.com.

13. Retaining your Personal Data

- 13.1. We retain your Personal Data as long as it is required in order to fulfill the relevant purposes described in this Policy, as well as are required by applicable law.

- 13.2. We will cease to retain your Personal Data, or remove the means by which the Personal Data can be associated with particular individuals, as soon as:
- (a) the purpose for which that Personal Data was collected is no longer being served by its retention; and
 - (b) retention is no longer required by applicable laws, accounting, or business purposes.
- 13.3. Please note that certain laws may require us to retain records of your Personal Data (e.g., transactions or accounts) for a certain period of time even after you cease relationship with us.
- 13.4. To determine the appropriate retention period for Personal Data, we consider the amount, nature, and sensitivity of the Personal Data, the potential risk of harm from unauthorized use or disclosure of your Personal Data, the purposes for which we process your Personal Data and whether we can achieve those purposes through other means, and the applicable legal requirements and recommendations.
- 13.5. The retaining of Personal 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.

14. Your rights regarding your Personal Data

- 14.1. Data Subjects are provided with legal rights governing the use of their Personal Data.
- 14.2. Under certain circumstances, you have the following rights under data protection laws in relation to your Personal Data:
- Request access to your Personal Data (commonly known as a “data subject access request”). This enables you to receive a copy of the Personal Data we hold about you and to check that we are lawfully processing it.
 - Request correction of the Personal Data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
 - Request erasure of your Personal Data. This enables you to ask us to delete or remove Personal Data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your Personal Data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your Personal Data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
 - Object to processing of your Personal Data where we are relying on a legitimate interest (or those of a third party) and there is something about your situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your Personal Data for

direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

- Request restriction of processing of your Personal Data. This enables you to ask us to suspend the processing of your Personal Data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- Request the transfer of your Personal Data to you or to a third party. We will provide to you, or a third party you have chosen, your Personal Data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- Withdraw consent at any time where we are relying on consent to process your Personal Data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent;
- Not to be the subject only to automated processing, including profiling. You have a right to demand that processing of your Personal Data would be reviewed by a real person and to object to the decision made by automated means.
- To submit an appeal on the actions or inactions of us, related to the implementation of the data subject's rights to the Data Protection authority that is located in member state of the European Union where you reside; and
- You are entitled to compensation, which you must apply for to the competent court that is located in member state of the European Union where you reside, if you have suffered damage as a result of a violation of the data subject's rights.

14.3. Please note that notwithstanding the foregoing, there may be circumstances in which we are unable to accommodate a request to edit, update, access, or delete an account profile or Personal Data. This includes but is not limited to:

- any basis where such request can be denied under applicable law;
- where we need to retain the information to comply with international or national laws or for accounting or tax purposes;
- where we need to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by state, or local authorities;
- where we need to cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate laws;
- where we need to retain information to exercise or defend legal claims;

- where the information contains legal privilege or proprietary information of another party; or where complying with the request would compromise others' privacy or other legitimate rights.
- 14.4. If we determine that we cannot respond to any request in any particular instance, we will provide you with an explanation of why that determination has been made and a contact point for any further inquiries. To protect your privacy, we will take commercially reasonable steps to verify your identity before responding to any request under this provision, including complying with any applicable legal requirement for verifying your identity.
- 14.5. We will respond to your requests without undue delay and in any event within one month of receipt of the request. However, period may be extended up to two months as per circumstances designated by GDPR.
- 14.6. You can also complain to the State Data Protection Inspectorate if you are unhappy with how we have used your data. We would, however, appreciate the chance to deal with your concerns before you approach the State Data Protection Inspectorate so, please contact us in the first instance.

The State Data Protection Inspectorate's address:

L. Sapiegos str. 17, LT-10312 Vilnius, Lithuania.

Email: ada@ada.lt.

Website: <https://vdai.lrv.lt/en/>

15. Protecting your Personal Data

- 15.1. We take all appropriate technical, physical and organizational steps to protect the confidentiality, integrity, availability and authenticity of your Personal Data, including when sharing your Personal Data to third parties. We implemented appropriate technical and organizational security 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.
- 15.2. We build security into our services to protect your information. All our products are built with strong security features that continuously protect your Personal Data. 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.
- 15.3. We regularly review this Policy and make sure that we process your information in ways that comply with it.
- 15.4. The User is responsible for providing the confidentiality of passwords, user names other information about access to Personal account and Platform.

- 15.5. The User is 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 User 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 User, the Company is not responsible for information security and safety. Company should be immediately notified if you becomes aware of unauthorized use or access of your account or user credentials.
- 15.6. The Company guarantees the confidentiality of Users 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.

16. Data Protection Officer

- 16.1. To ensure data privacy and protection has appropriate focus within our organization we have appointed a Data Protection Officer (DPO). The contact details can be found at the end of this Policy.

17. Data Protection of using digital assets and blockchains

- 17.1. Your use of digital assets may be recorded on a public blockchain. Public blockchains are distributed ledgers, intended to immutably record transactions across wide networks of computer systems. Many blockchains are open to forensic analysis which can lead to re-identification of transacting individuals and the revelation of Personal Data, especially when blockchain data is combined with other data.
- 17.2. As blockchains are decentralized or third-party networks which are not controlled or operated by the Company, we are not able to erase, modify, or alter Personal Data on such networks.

18. Third-Party Links

- 18.1. Our Platform may contain links to third-party websites. Any access to and use of such linked websites is not governed by this Policy, but instead is governed by the privacy policies of those third-party websites. We are not responsible for the information practices of such third-party websites.

19. Children Under 18

- 19.1. Our Services are not intended for the use of children under 18. If we discover that a child under 18 has provided us with Personal Data, we will delete such information from our systems, unless it is required otherwise by applicable law.

20. Complaints

- 20.1. If you are dissatisfied with any aspect on how we process your Personal Data please contact our DPO by emailing info@columis.com.

21. How To Contact Us

- 21.1. If you have any questions regarding this Policy and its content, the use of your data and your data subject rights, please contact our DPO at Columis address or by emailing info@columis.com.

22. Changes to this Policy

- 22.1. This Policy is current as of the Last Update Date set forth below. We may change this Policy from time to time, so please be sure to check back periodically. We will post any changes to this Policy on the Platform. If we make any changes to this Policy that materially affect our practices with regard to the Personal Data we have previously collected from you, we will endeavor to provide you with notice in advance of such change by highlighting the change on our Platform or providing a push notification through the Website (you should make sure your Website settings allow for such push notifications) or sending an email that you have provided in your account, (for this reason you should make sure to update your account information promptly if it changes).

LAST UPDATE DATE: 27 February, 2025