

## **PRIVACY POLICY**

Last Updated: October 2023

Zimbro., a Cayman Islands exempted company, UAB Star Ventures (“Star Ventures”), a company incorporated and existing under the laws of Lithuania and Nebula Ventures Ltd. (“Nebula”), a company incorporated and existing under the laws of the Seychelles, their respective direct and indirect subsidiaries and affiliates and any entities under common control with Zimbro., Star Ventures or Nebula (collectively, “Zimbro”, “we”, “us” and “our”) take data protection and security seriously. This Privacy Policy describes how we collect and process your personal data when you access content we own or operate on the website located at [www.zimbro.app](http://www.zimbro.app) (the “Website”) or on any other websites, pages, features, content or applications we own or operate (collectively, the “Other Sites” together with the “Website”, the “Zimbro”) and/or when you use any of our APIs or third party applications relying on such APIs, and any of our respective products or services (referred to collectively hereinafter as our “Services”). This Privacy Policy is incorporated by reference and forms part of the Zimbro User Agreement.

Please read this Privacy Policy carefully and its entirety. If you have any questions about this Privacy Policy, please contact us at [privacy@zimbro.app](mailto:privacy@zimbro.app).

### **ACCEPTANCE OF PRIVACY POLICY**

By accessing and using the Zimbro or our Services, you acknowledge that you have read, understand, and agree to all of the terms and conditions contained in this Privacy Policy. If you do not agree with or are not comfortable with any aspect of this Privacy Policy, you should immediately discontinue access or use of the Zimbro and our Services.

### **CHANGES TO THIS PRIVACY POLICY**

We reserve the right to alter, amend or modify this Privacy Policy from time to time, in our sole discretion. We will provide you with notice of such changes by sending an e-mail, providing notice on the homepage of the Website and/or by posting the amended Privacy Policy via our Website and updating the “Last Updated” date at the top of this Privacy Policy. The amended Privacy Policy will be deemed effective immediately upon posting on the Website. Your continued use of the Zimbro and/or our Services constitutes your agreement to be bound by any such changes to this Privacy Policy. If you do not agree with this Privacy Policy or any amendment to it, you should discontinue access and use of the Zimbro and our Services.

### **DATA WE COLLECT**

When you visit the Zimbro, you may provide us with two types of information: personal data that you voluntarily disclose or that is collected on an individual basis; and information collected automatically when you use the Zimbro or our Services including, without limitation, information that we obtain from our partners (collectively, the “Information”).

We will only collect and process Information for specified and lawful purposes and only to the extent it is appropriate and necessary for one or more of the purposes outlined in this Privacy Policy, namely for the purpose of providing Services and information about our Services to you and/or to comply with legal requirements. You may be asked to provide personal data anytime you are in contact with us. Any information you provide to us that is not required is voluntary. You are free to choose whether to provide us with the types of personal data requested, but we may not be able to serve you as effectively or offer you all our Services if you choose not to share certain information with us.

## **Personal Data**

Personal data is any information which is related to an identified or identifiable natural person. This 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 it cannot be used to identify you. Personal data means any information that is unique to you, such as your:

- full legal name, date of birth, age, nationality, gender, signature, utility bills, phone number, email address and home address;
- passport or other photo identification such as a driver's license or national identification card, other photographs like selfies;
- biometric data for verification and identification purposes;
- user ID, security questions, authentication data, transaction information, financial information, digital currency, or wallet addresses; and
- other personal data you may choose to provide us.

With your permission, we may also access other personal data on your device, such as your phone book, calendar, or messages, in order to provide Services to you. If authorized by you, we may also access profiles and other information from services like Facebook.

We may also collect and obtain information about you to comply with our legal obligations, such as anti-money laundering laws. We may obtain information about you from third party sources as required or permitted by applicable law, such as public databases, credit bureaus, ID verification partners, channel partners, joint marketing partners, and social media platforms. For example, we obtain information about you from public databases and ID verification partners for purposes of verifying your identity when you sign up for our Services or use our Services. Our 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 sanction lists maintained by public authorities, and other relevant data. Pursuant to applicable data protection laws, our lawful basis for processing such data is compliance with our legal obligations. In some cases, we may process additional data about you to ensure our Services are not being used fraudulently or for other illicit activities.

By using our Services or providing us with your personal data, you also expressly consent for us to collect, hold, use and disclose your personal data in accordance with this Privacy Policy and our User Agreement. In addition to providing the foregoing information, if you choose to correspond further with us through e-mail or through the "contact" section of the Zimbros or through events and public social networking platforms, we may retain, use, and disclose the content of your messages together with your user ID and e-mail address and our responses.

You are required to advise us of any changes in your personal data that may impact the Services we are providing. From time to time, you may be asked to verify or update your personal data.

### **Information that is Collected Automatically**

When you use Zimbro or our Services, we automatically collect information from your devices. We collect the following information:

- **Server Log Information:** We collect server log information when you use the Zimbro, which may include (but is not limited to) your login details, the date and time of visits, the pages viewed, your IP address, time spent at the Zimbro and the websites you visit just before and just after the Website.
- **Device Information:** We collect information about the computer or mobile device you use to access the Zimbro, including the hardware model, geo location/tracking details, browser fingerprint, operating system and version, the web browser and version you use, and other device identifiers.
- **Telemetry Information.** If you use any of our open-source software, we may collect bandwidth download and upload speeds, the amount of free and used storage space on your device and other statistics about your device.
- **Usage Information.** If you use the Zimbro, we will collect metadata about the files you upload for storage and information about the transactions you make on the Zimbro or with our Services, such as the name of recipients, your name, digital asset amounts, click-stream data, instances in which you have used your private key to authenticate communications and/or the timestamp of transactions.
- **Information Collected by Cookies and Other Tracking Technologies:** We and our service providers use various technologies to collect information when you interact with the Zimbro, including cookies, web beacons and other unique device identifiers. Cookies are small data files that are stored on your device when you visit a website, which enable us to collect information about your device, IP address, web browsers used to access the Zimbro, pages or features viewed, time spent on pages, mobile app performance and links clicked. Web beacons are graphic images that are placed on a website or in an email that is used to monitor the behavior of the user visiting the website or sending the email. They are often used in combination with cookies.

### **HOW YOUR PERSONAL DATA IS USED**

The primary purpose for collecting your Information is to provide you with the best possible user experience and Services and to safeguard the security and stability of our systems. In general, we use Information to create, develop, operate, deliver, and improve our Services, content, and marketing, to comply with our legal obligations, for anti-fraud purposes and for loss prevention. Specifically, we will process your Information on the following bases and for the following purposes:

- to provide, maintain, deliver or improve the Zimbrow or our Services;
- for quality control and staff training including improving our existing Services to ensure we can provide you with the best user experience and accurate information;
- to monitor and analyze trends, usage and activities in connection with the Zimbrow, to determine the usefulness or popularity of certain content and to better understand the online activity of users of the Zimbrow;
- to ensure our compliance with all relevant legal or regulatory requirements and to meet our regulatory and legal obligations;
- to assess risks including legal and financial risks;
- it is necessary for us to perform a task in the public interest;
- to enforce the terms and conditions of our [User Agreement](#) and other agreements we may have with you or third parties including, without limitation, if we believe your actions are inconsistent with our [User Agreement](#), our other agreements or policies;
- it is necessary for, or to protect, our interests, rights, property and safety, or that of others;
- to ensure network and information security including processing your Information in order to enhance security, monitor and verify identity or service access, combat spam or other malware or security risks and to comply with applicable security laws and regulations;
- in accordance with your consent including providing you with the information or products or services that you have requested;
- to monitor and manage the performance of our business operations, to analyze performance and generate internal reports;
- to invoice and process payments;
- to manage, maintain and develop our relationship with you and provide you with customer service including, without limitation, answering your inquiries or responding to a communication from you;
- for research and development purposes including developing new products or services;
- to send you technical notices, support or administrative notifications;
- to facilitate marketing and to communicate with you about news, products, services,

events and other information we think will be of interest to you;

- in order to detect, investigate and prevent fraud or other illegal or unauthorized transactions or activities;
- to facilitate the effective management and administration of our business, including in relation to matters such as business planning, budgeting, and forecasting;
- to facilitate reorganization, an asset or business sale, corporate acquisitions, mergers, or other transactions;
- to link, connect or combine Information we collect from or about you with other Information; and
- to carry out any other purpose or reason for which the Information was collected, for which we have received your consent or for which we or our third parties have a legitimate interest.

For each of the purposes for which we process information, we rely on the following legal justifications:

- Contractual Necessity** – we rely on this justification where we process your personal data in order to discharge contractual obligations we owe you for the purpose of service delivery.
- Legitimate Business Interest** – we rely on this justification where we need to process your personal data in order to meet our own requirement to operate, manage, and develop our business or to safeguard the legitimate interests pursued by us or by a third party (provided there is a balance between your interests and our interests). A legitimate interest is when we have a business or commercial reason to use your information.
- Legal and Regulatory Requirement** – we rely on this justification where we use your Information for the purpose of legal and regulatory compliance. We do this not only to comply with our legal obligations but because it may also be in our legitimate interest to do so.
- Legal Proceedings** – we rely on this justification where it is necessary to handle your Information for the purpose of obtaining legal advice; in connection with any legal proceeding; or to exercise or defend legal rights in accordance with applicable data protection legislation.
- Consent** – we use your Information based on your consent.

## SHARING OF INFORMATION

We will never sell or rent your personal data. We will only share your Information if and to the extent appropriate or necessary to do so for one or more of the purposes outlined in this Privacy Policy or our User Agreement and will ensure that the sharing of such Information is kept to the minimum necessary. To the extent we share your Information will vary depending on your circumstances and your relationship with us, but we may share your Information with one or more of the following categories of recipients:

other members or associates of your organization;

with our current or future parent companies, affiliates, subsidiaries and with other companies under common control or ownership with us or our offices internationally;

with advisors, sub-contractors, consultants, agents, service providers or other third parties that we have partnered with or perform work for us and those who support our business operations;

those who provide ancillary services which complement the Services we provide;

to users of interactive areas of the Zimbros or our social media platforms like our online forums if you choose to share or display your personal data on them publicly, such as your username and any content you post;

to third parties, advisors, agents and other service providers in connection with a reorganization, change of ownership, merger or transfer of all or part of our assets or business, or if we do a financing or are involved in an acquisition or any other situation where Information may be disclosed or transferred as one of our business assets;

with government departments and agencies, law enforcement officials, regulators, courts, tribunals or other third parties when we are compelled to do so by a subpoena, court order, or similar legal procedure or request, or when we believe in good faith that the disclosure of Information is necessary to prevent physical harm or financial loss, to report suspected illegal activity, to investigate violations of this Privacy Policy, our [User Agreement](#) or any other applicable policies or if we believe disclosure is in accordance with, or required by, any applicable law, regulation or legal process; and

with third parties where aggregate Information is disclosed which cannot reasonably be used to identify you.

We use reasonable efforts to ensure that third parties we partner with are bound by the terms of this Privacy Policy or a similar policy. Your Information may be transferred to or accessed by the

recipients described above from countries located anywhere in the world. Such countries may have different and potentially less stringent standards relating to data protection than your country. In these cases, we will, whenever possible, take all appropriate steps that are within our control to ensure that adequate legal safeguards are in place for your personal data which are shared with such recipients. By using our Services, you consent to your Information being transferred to other countries, including countries that have differing levels of privacy and data protection laws than your country. In all such transfers, we may rely on standard contractual clauses and will protect and process your personal data as described in this Privacy Policy.

## **SOCIAL SHARING FEATURES**

Zimbro may offer social sharing features, links to social media and other integrated tools. Your use of such features enables the sharing of information with your contacts or the public, depending on the settings you use with the entity that provides the social sharing feature or social media. Please visit the privacy policies of the entities that provide these features to obtain more information about the purpose and scope of data collection and the processing of such data by such entities.

## **HYPERLINKS AND THIRD-PARTY SITES**

The Zimbro may contain links to other third-party websites that may collect personal data about you, including through cookies or other technologies. If you link to another website, you will leave the Zimbro and this Privacy Policy will not apply to your use of and activity on those other websites. You should consult these other websites' privacy policies as we have no control over them and are not responsible for any information that is submitted to or collected by these third parties.

## **PRIVACY WHEN USING DIGITAL ASSETS AND BLOCKCHAINS**

Your transactions involving bitcoin, ether and other digital currency or virtual 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 deanonymization and the unintentional revelation of private financial information, especially when blockchain data is combined with other data.

Because blockchains are decentralized or third-party networks which are not controlled or operated by use, we are not able to erase, modify, or alter personal data from such networks.

## **MARKETING AND ONLINE COMMUNICATION**

We require your consent to send you marketing communications (for example: email marketing, exclusive offers, etc).

If you are a *new* customer, we will contact you by electronic means (email or SMS) for marketing purposes only if you have consented to such communication. If you are a *current* customer, we will only contact you by electronic means with information about our Services that are similar to those which were the subject of a previous sale or negotiations of a sale to you.

If you do not want us to use your personal data for direct marketing purposes or to pass your personal data on to third parties for marketing purposes, you can withdraw your consent by



logging into your account at [www.zimbro.app](http://www.zimbro.app) or by contacting us at [privacy@zimbro.app](mailto:privacy@zimbro.app). Direct marketing includes any communications to you that are only based on advertising or promoting products and services.

As mentioned above, you can opt out of our marketing communications anytime. However, certain electronic communications between us and you are necessary for usage of our Services including

login notifications, withdrawal confirmations, deposit notifications and 2-Factor Authentication (this can be replaced with Google Authenticator, Authy, or Trezor). We highly recommend that you do not turn off 2-Factor Authentication as this provides the maximum amount of security for your account.

If you chose not to consent to the terms of this Privacy Policy or opt out of receiving notifications from us that makes it difficult or impractical for us to provide Services to you, we will grant you a period of up to 10 business days from the moment you do not consent or opt out to move your assets to an external digital wallet of your choosing and close your account.

## **PROTECTION OF PERSONAL DATA**

We take reasonable administrative, physical and electronic measures designed to safeguard and protect your personal data from unauthorized access or disclosure. This includes utilizing Secure Sockets Layer (SSL) software, which encrypts the personal data you input, and storing your personal data in encrypted form behind a firewall designed to block access from outside our network. However, no security or encryption method can be guaranteed to protect information from hackers or human error, no computer security system is entirely fool-proof, and the Internet is not a secure method of transmitting information. As a result, we do not assume any responsibility for the data you submit to or receive from us through the Internet or for any unauthorized access or use of that information and we cannot and do not guarantee that personal data communicated by you to us or sent to you by us will be received or that it will not be altered before or after its transmission to us.

We cannot guarantee that loss, misuse, unauthorized acquisition, or alteration of your Information will not occur. Please recognize that you play a vital role in protecting your own Information. When providing information on the Zimbro or accessing or using our Services, you should choose a password of sufficient length and complexity, not reveal this password to any third parties, and to immediately notify us if you become aware of any unauthorized access to or use of your account.

Furthermore, we cannot ensure or warrant the security or confidentiality of Information you transmit to us or receive from us by Internet or wireless connection, including email, phone, or SMS, since we have no way of protecting that Information once it leaves and until it reaches us. If you have reason to believe that your data is no longer secure, please contact us at [privacy@zimbro.app](mailto:privacy@zimbro.app).

## **RETENTION PERIOD OF DATA**

Information we collect may be stored or processed on computers located in any country where we provide Services or carry on business. We will only retain your personal data for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting obligations or to resolve disputes. This is a case-by-case determination that depends on things such as the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, we may retain certain information for accounting and security purposes even after our business relationship with you has ceased.

## **RIGHTS YOU HAVE WITH RESPECT TO YOUR PERSONAL DATA**

You have certain individual rights regarding the personal data that we collect and process about you through the Zimbro.

Most web browsers are set to accept cookies as a default. You may wish to opt out by turning off cookies (please refer to the help menu on your browser); however, switching off cookies may restrict your use of the Zimbro.

As mentioned, you may also opt out of receiving promotional communications from us at any time by following the instructions in those communications. If you opt out, we may still send you non- promotional communications, such as technical notices, support or administrative notifications or information about your account (if you have one).

Pursuant to applicable data protection laws, you may have certain legal rights in respect of the personal data which is processed by us including the right to:

- access or receive certain data about the personal data we process about you;

- have your personal data corrected, updated, rectified or deleted;

- object to the processing of your personal information or ask us to restrict processing of your personal data;

- withdraw your consent to our processing of your personal data; and

- not be subject to a decision based solely on automated processing of your personal data, including profiling, which produces legal or similarly significant effects on you, save for the exceptions applicable under relevant data protection laws.

If applicable data protection laws apply, you may also have the right to receive a copy of your personal data in a structured, commonly used and machine-readable format for the purpose of transferring such information to a third party subject to a reasonable fee associated with the work required by us to gather the information.

Please note, however, that your rights are subject to certain exceptions and conditions. Specifically, we may need to further process and retain your Information to perform a contract with you or your company or organization, to protect our legitimate interests (such as the establishment, exercise or defense of legal claims) or to comply with legal requirements. To the extent permitted by law, namely, to protect the rights and freedoms of others or to protect our own legitimate interests, we may therefore refuse to satisfy your request or we may satisfy your request only on a restricted basis.

You may withdraw your consent to the processing of your Information. However, if there is another legitimate basis for processing your Information, the Information may be processed without your consent.

Lastly, you have a right to lodge a complaint with a competent supervisory authority.

If you wish to exercise any of your rights, you should contact us at [privacy@zimbro.app](mailto:privacy@zimbro.app).

## **CHILDREN'S PERSONAL DATA**

We do not knowingly collect personal data from any person under the age of 18. If a user submitting personal data is suspected of being younger than 18 years of age, we will require the user to close his or her account and will not allow the user to continue to use our Services. We will also take steps to delete the Information as soon as possible. Please notify us if you or anyone you know is under the age of 18 and are using our Services so we can take action to prevent access to our Services.

## **HOW TO CONTACT US**

If you have questions or concerns regarding this Privacy Policy or if you have a complaint, please contact us at [privacy@zimbrowapp.com](mailto:privacy@zimbrowapp.com). If we are unable to satisfactorily address your concerns, you have the right to communicate with a relevant supervisory authority. We can direct you to the relevant supervisory authority in your jurisdiction.