Privacy Policy

Last Updated Date: Wed April 16, 2025

River Eridanus Association ("**Association**", "**we**", "**us**" or "**our**") offers the Towns Protocol and associated services. This Privacy Policy describes how we process personal information that we collect through our digital or online properties or services that link to this Privacy Policy (including as applicable, our websites (such as towns.com, gov.towns.com), and social media pages) as well as our marketing activities, live events and other activities described in this Privacy Policy (collectively, the "**Service**"). At or before the time we collect personal information, the Association may provide additional or supplemental privacy policies for specific products or services that we offer.

European Users: Please see the 'Notice to European Users' section below for additional information for individuals located in Switzerland, the European Economic Area, or the United Kingdom (which we refer to as "**Europe**", and "**European**" should be understood accordingly) below.

Personal information we collect

Information you provide to us. Personal information you may provide to us through the Service or otherwise includes:

- **Profile data gov.towns.com,** such as wallet address, username and password you may set to establish an account on the Service, photograph or picture, and any other information that you add to your account profile.
- **Contact data gov.towns.com,** such as your first and last name and email address.
- **User-generated content data gov.towns.com**, such as comments, questions, messages, reviews, reactions, responses and other content or information that you generate, transmit, or otherwise make available on the Service, as well as associated metadata. Metadata includes information on how, when, where and by whom a piece of content was collected and how that content has been formatted or edited. Metadata also includes information that users can add or can have added to their content, such as keywords, geographical or location information, and other similar data.
- **Grant application data**, such as your company name, project description, and budget when you apply for a grant with us.
- **Transactional data**, such as your blockchain transaction history and other information associated with your linked cryptocurrency wallet, information relating to or needed to complete your transactions on or through the Service (such as your wallet address), account balances, token holdings, transaction number, transaction amount, as well as information relating to or needed to claim an airdropped token or complete your staking request.
- **Financial data**, such as your virtual currency or wallet account balances and other associated information.
- **Communications data** based on your communications with other Service users as well as our exchanges with you (including when you contact us through the Service, social media, or otherwise).
- **Marketing data**, such as your preferences for receiving our marketing communications and details about your engagement with them.
- **Other data** not specifically listed here, which we will use as described in this Privacy Policy or as otherwise disclosed at the time of collection.

Third-party sources. We may combine personal information we receive from you with personal information falling within one of the categories identified above that we obtain from other sources, such as:

- **Public sources**, such as government agencies, public records (such as publicly-available blockchains), social media platforms, and other publicly available sources.
- **Data providers,** such as information services and data licensors.
- **Partners**, such marketing partners and event co-sponsors.
- **Business transaction partners.** We may receive personal information in connection with an actual or prospective business transaction. For example, we may receive your personal information from an entity we acquire or are acquired by, a successor, or assignee or any party involved in a business transaction such as a merger, acquisition, sale of assets, or similar transaction, or in the context of an insolvency, bankruptcy, or receivership.
- **Third-party services**, such as virtual currency account services or social media services that you use to log into, or otherwise link to, your Service account. This data may include your username, profile picture, wallet address, and other information associated with your account on that third-party service that is made available to us based on your account settings on that service.

Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as:

- **Device data**, such as your computer or mobile device's operating system type and version, manufacturer and model, browser type, screen resolution, RAM and disk size, CPU usage, device type (e.g., phone, tablet), IP address, unique identifiers (including identifiers used for advertising purposes), language settings, mobile device carrier, radio/network information (e.g., Wi-Fi, LTE, 3G), and general location information such as city, state or geographic area.
- **Online activity data**, such as pages or screens you viewed, how long you spent on a page or screen, the website you visited before browsing to the Service, navigation paths between pages or screens, information about your activity on a page or screen, access times and duration of access, and whether you have opened our emails or clicked links within them.
- **Communication interaction data** such as your interactions with our email, text or other communications (e.g., whether you open or forward emails) – we may do this through use of pixel tags (which are also known as clear GIFs), which may be embedded invisibly in our emails.

For more information concerning our automatic collection of data, please see the Tracking & Other technologies section below.

Tracking & Other Technologies

Cookies and other similar technologies. Some of the automatic collection described above is facilitated by the following technologies:

- **Cookies**, which are small text files that websites store on user devices and that allow web servers to record users' web browsing activities and remember their submissions, preferences, and login status as they navigate a site. Cookies used on our sites include both "session cookies" that are deleted when a session ends, "persistent cookies" that remain longer, "first party"

cookies that we place and “third party” cookies that our third-party business partners and service providers place.
- **Local storage technologies**, like HTML5, that provide cookie-equivalent functionality but can store larger amounts of data on your device outside of your browser in connection with specific applications.
- **Web beacons**, also known as pixel tags or clear GIFs, which are used to demonstrate that a webpage or email was accessed or opened, or that certain content was viewed or clicked.
- **Session-replay technologies**, such as those provided by MixPanel and Instabug that employ software code to record users’ interactions with the Services in a manner that allows us to watch video replays of those user sessions. The replays include users’ clicks, mobile app touches, mouse movements, scrolls and keystrokes/key touches during those sessions. These replays help us diagnose usability problems and identify areas for improvement. You can learn more about Mixpanel at https://mixpanel.com/legal/privacy-policy and about Instabug at https://www.instabug.com/privacy.

For information concerning your choices with respect to the use of tracking technologies, see the **Your choices** section, below.

How we use your personal information

We may use your personal information for the following purposes or as otherwise described at the time of collection:

Service delivery and operations. We may use your personal information to:
- provide the Service and operate our business;
- enable security features of the Service;
- establish and maintain your profile on the Service;
- communicate with you about the Service, including by sending Service-related announcements, updates, security alerts, and support and administrative messages;
- communicate with you about events or contests in which you participate; and
- provide support for the Service, and respond to your requests, questions and feedback.

Service personalization, which may include using your personal information to:
- understand your needs and interests;
- personalize your experience with the Service and our Service-related communications; and
- remember your selections and preferences as you navigate webpages.

Service improvement and analytics. We may use your personal information to analyze your usage of the Service, improve the Service, improve the rest of our business, help us understand user activity on the Service, including which pages are most and least visited and how visitors move around the Service, as well as user interactions with our emails, and to develop new products and services. For example, we use Mixpanel for this purpose. You can learn more about Mixpanel at https://mixpanel.com/legal/privacy-policy.

Marketing. We and our service providers may collect and use your personal information for direct marketing purposes. We may send you direct marketing communications and may personalize these messages based on your needs and interests.

Events. We may use your personal information to:

- administer and communicate with you about events in which you participate; and
- contact or market to you after collecting your personal information at an event.

Compliance and protection. We may use your personal information to:

- comply with applicable laws, lawful requests, and legal process, such as to respond to subpoenas, investigations or requests from government authorities;
- protect our, your or others' rights, privacy, safety or property (including by making and defending legal claims);
- audit our internal processes for compliance with legal and contractual requirements or our internal policies;
- enforce the terms and conditions that govern the Service; and
- prevent, identify, investigate and deter fraudulent, harmful, unauthorized, unethical or illegal activity, including cyberattacks, identity theft, and sanctions screening.

Data sharing in the context of corporate events. We may share certain personal information in the context of actual or prospective corporate events – for more information, see How we share your personal information, below.

To create aggregated, de-identified or anonymized data. We may create aggregated, de-identified or anonymized data from your personal information and other individuals whose personal information we collect. We make personal information into de-identified or anonymized data by removing information that makes the data identifiable to you. We may use this aggregated, de-identified or anonymized data and share it with third parties for our lawful business purposes, including to analyze and improve the Service and promote our business.

Further uses. In some cases, we may use your personal information for further uses, in which case we will ask for your consent to use of your personal information for those further purposes if they are not compatible with the initial purpose for which information was collected.

Cookies and other similar technologies. In addition to the other uses included in this section, we may use the **Tracking & Other Technologies** described above for the following purposes:

- **Technical operation**. To allow the technical operation of the Service, such as by remembering your selections and preferences as you navigate the site and mobile app, and whether you are logged in when you visit password protected areas of the Service.
- **Functionality**. To enhance the performance and functionality of our services.
- **Analytics**. To help us understand user activity on the Service, including which pages are most and least visited and how visitors move around the Service, as well as user interactions with our emails.

Retention

We generally retain personal information to fulfill the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements, to establish or defend legal claims, or for fraud prevention purposes. To determine the appropriate retention period for personal information, we may consider factors such as the amount, nature, and sensitivity of the personal

information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

When we no longer require the personal information we have collected about you, we may either delete it (where possible), anonymize it, or isolate it from further processing.

How we share your personal information

We may share your personal information with the following parties (or as otherwise described in this Privacy Policy, in other applicable notices, or at the time of collection).

Affiliates. Our corporate parent, subsidiaries, and affiliates.

Service providers. Third parties that provide services on our behalf or help us operate the Service or our business (such as hosting, information technology, customer support, email delivery, marketing, consumer research and website analytics).

Cryptocurrency platforms. We may share your personal information, such as information to link your virtual wallet to the Services and information about your activities on the Services, with your chosen cryptocurrency platform, such as MetaMask or Coinbase Wallet. Please review the privacy policies for the relevant cryptocurrency platform to learn how they may use your personal information. For example, MetaMask's privacy policy is available at https://consensys.net/privacy-policy/, and Coinbase Wallet's privacy policy is available at https://www.coinbase.com/legal/privacy.

Linked third-party services. If you log into the Service with, or otherwise link your Service account to, a virtual currency account, social media or other third-party service, we may share your personal information with that third-party service. The third party's use of the shared information will be governed by its privacy policy and the settings associated with your account with the third-party service.

Third parties designated by you. We may share your personal information with third parties where you have instructed us or provided your consent to do so.

Professional advisors. Professional advisors, such as lawyers, auditors, bankers and insurers, where necessary in the course of the professional services that they render to us.

Authorities and others. Law enforcement, government authorities, and private parties, as we believe in good faith to be necessary or appropriate for the Compliance and protection purposes described above.

Business transferees. We may disclose personal information in the context of actual or prospective business transactions (*e.g.,* investments in or financing of us, public stock offerings, or the sale, transfer or merger of all or part of our business, assets or shares). For example, we may need to share certain personal information with prospective counterparties and their advisers. We may also disclose your personal information to an acquirer, successor, or assignee of us as part of any merger, acquisition, sale of assets, or similar transaction, or in the event of an insolvency, bankruptcy, or receivership in which personal information is transferred to one or more third parties as one of our business assets.

Other users and the public. Your profile and other user-generated content data are visible to other users of the Service and the public. For example, other users of the Service or the public may have access to your information if you chose to make your profile or other personal information available to them through the Service, such as when you participate in the forum on gov.towns.com by reading, writing, and evaluating content shared. Due to the nature of blockchain technologies, any data posted to a blockchain will be visible to other users of the Service and the public. This information can be seen, collected and used by others, including being cached, copied, screen captured or stored elsewhere by others (e.g., search engines), and we are not responsible for any such use of this information.

Your choices

Access or update your information. If you have registered for an account with us through the Service, you may review and update certain account information by logging into the account and accessing your profile.

Cookies and other technologies. Most browsers let you remove or reject cookies. To do this, follow the instructions in your browser settings. Many browsers accept cookies by default until you change your settings. Please note that if you set your browser to disable cookies, the Service may not work properly. For more information about cookies, including how to see what cookies have been set on your browser and how to manage and delete them, visit www.allaboutcookies.org. You can also configure your device to prevent images from loading to prevent web beacons from functioning.

Blocking images/clear gifs: Most browsers and devices allow you to configure your device to prevent images from loading. To do this, follow the instructions in your particular browser or device settings.

Do Not Track. Some Internet browsers may be configured to send "Do Not Track" signals to the online services that you visit. We currently do not respond to "Do Not Track" signals. To find out more about "Do Not Track," please visit http://www.allaboutdnt.com.

Declining to provide information. We need to collect personal information to provide certain services. If you do not provide the information we identify as required or mandatory, we may not be able to provide those services.

Linked third-party platforms. If you choose to connect to the Service through your virtual currency account, social media account or other third-party platform, you may be able to use your settings in your account with that platform to limit the information we receive from it. If you revoke our ability to access information from a third-party platform, that choice will not apply to information that we have already received from that third party.

Other sites and services

The Service may contain links to websites, mobile applications, and other online services operated by third parties. In addition, our content may be integrated into web pages or other online services that are not associated with us. These links and integrations are not an endorsement of, or representation that we are affiliated with, any third party. We do not control websites, mobile applications or online services

operated by third parties, and we are not responsible for their actions. We encourage you to read the privacy policies of the other websites, mobile applications and online services you use.

Security

We employ technical, organizational and physical safeguards designed to protect the personal information we collect. However, security risk is inherent in all internet and information technologies, and we cannot guarantee the security of your personal information.

International data transfer

We are headquartered in Switzerland and may use service providers that operate in other countries. Your personal information may be transferred to the United States or other locations where privacy laws may not be as protective as those in your state, province, or country.

Users in Europe should also read the information provided about transfers of personal information to recipients outside Europe contained in the 'Notice to European users' below.

Children

The Service is not intended for use by anyone under 18 years of age. If you are a parent or guardian of a child from whom you believe we have collected personal information in a manner prohibited by law, please contact us. If we learn that we have collected personal information through the Service from a child without the consent of the child's parent or guardian as required by law, we will comply with applicable legal requirements to delete (where possible) the information.

Changes to this Privacy Policy

We reserve the right to modify this Privacy Policy at any time. If we make material changes to this Privacy Policy, we will notify you by updating the date of this Privacy Policy and posting it on the Service or other appropriate means. Any modifications to this Privacy Policy will be effective upon our posting the modified version (or as otherwise indicated at the time of posting). In all cases, your use of the Service after the effective date of any modified Privacy Policy indicates your acknowledging that the modified Privacy Policy applies to your interactions with the Service and our business.

How to contact us

If you have questions about our practices or if you would like to exercise any privacy related right that may be available to you, please contact us via the method listed below.

- **Email**: help@towns.com

Notice to European Users

General

Where this Notice to European users applies. The information provided in this "Notice to European users" section applies only to individuals in Switzerland, the European Economic Area, and the United Kingdom (i.e., "**Europe**" as defined at the top of this Privacy Policy).

Personal information. References to "personal information" in this Privacy Policy should be understood to include a reference to "personal data" (as defined in the GDPR and the FADP) – i.e., information about individuals from they are either directly identified or can be identified.

Controller. The Association is the controller in respect of the processing of your personal information covered by this Privacy Policy for purposes of European data protection legislation (i.e., the EU GDPR and the so-called 'UK GDPR' (as and where applicable, the "GDPR")) and the Swiss Federal Act on Data Protection (as and where applicable, the "**FADP**"). See the 'How to contact us' section above for our contact details.

Our legal bases for processing

In respect of each of the purposes for which we use your personal information, the GDPR requires us to ensure that we have a "legal basis" for that use.

Our legal bases for processing your personal information described in this Privacy Policy are listed below.

- Where we need to perform a contract, we are about to enter into or have entered into with you ("**Contractual Necessity**").
- Where it is necessary for our legitimate interests and your interests and fundamental rights do not override those interests ("**Legitimate Interests**"). More detail about the specific legitimate interests pursued in respect of each Purpose we use your personal information for is set out in the table below.
- Where we need to comply with a legal or regulatory obligation ("**Compliance with Law**").
- Where we have your specific consent to carry out the processing for the Purpose in question ("**Consent**").

We have set out below, in a table format, the legal bases we rely on in respect of the relevant Purposes for which we use your personal information – for more information on these Purposes and the data types involved, see 'How We Use Your Personal Information'.

Purpose	Categories of personal information involved	Legal basis
Service delivery and operations	• Contact data • Profile data • User-generated content data • Grant application data • Transactional data • Financial data • Communications data • Data from Third Party Services • Device data	• **Contractual Necessity**. • **Legitimate Interests**. We have a legitimate interest in ensuring the ongoing security and proper operation of our Service (including, where relevant, responding to any contact via any "contact us" feature or similar), our business and associated IT services, systems and networks.
Service personalization	• Contact data • Profile data • Communications data • Device data	• **Legitimate Interests.** We have a legitimate interest in providing you with a good service via the Service, which is personalized to you and that remembers your selections and preferences.
Service improvement and analytics	• Contact data • Device data • Online activity data	• **Legitimate Interests.** We have a legitimate interest in providing you with a good service and analysing how you use it so that we can improve it over time, as well as developing and growing our business.
Marketing	• Contact data • Communications data • Marketing data	• **Legitimate Interests**. We have a legitimate interest in promoting our operations and goals as an organisation and sending marketing communications for that purpose. • **Consent**, in circumstances or in jurisdictions where consent is required under applicable data protection laws to the sending of any given marketing communications.

Purpose	Categories of personal information involved	Legal basis
Events	● Contact data ● Communications data	● **Contractual Necessity**, to administer events in accordance with the terms or rules thereof (including communicating with you as and where necessary). ● In respect of promoting these events: o **Legitimate Interests** – we have a legitimate interest in promoting these events, including the associated publicising of our business and operations. o **Consent** – in circumstances or in jurisdictions where consent is required under applicable data protection laws to the sending of any given promotional communications.
Compliance and protection	Any and all data types relevant in the circumstances	● **Compliance with Law**. ● **Legitimate Interests**. Where Compliance with Law is not applicable, we have a legitimate interest in participating in, supporting, and following legal process and requests, including through co-operation with authorities. We may also have a legitimate interest of ensuring the protection, maintenance, and enforcement of our rights, property, and/or safety.
Corporate events	Any and all data types relevant in the circumstances	● **Legitimate Interests**. We have a legitimate interest in providing information to relevant third parties who are involved in an actual or prospective corporate event (including to enable them to investigate – and, where relevant, to continue to operate – all or relevant part(s) of our operations).
To create aggregated, de-identified and/or anonymized data	Any and all data types relevant in the circumstances	● **Legitimate Interests**. We have legitimate interest in taking steps to preserve the privacy of our users.
Further uses	Any and all data types relevant in the circumstances	● The original legal basis relied upon, if the relevant further use is compatible with the initial purpose for which the personal information was collected. ● Consent, if the relevant further use is not compatible with the initial purpose for which the personal information was collected.

Other info

No sensitive personal information. We ask that you not provide us with any sensitive personal information (e.g., social security numbers, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometrics or genetic characteristics, criminal background or trade union membership) on or through the services, or otherwise to us. If you provide us with any sensitive personal information to us when you use the services, you must consent to our processing and use of such sensitive personal information in accordance with this Privacy Policy. If you do not consent to our processing and use of such sensitive personal information, you must not submit such sensitive personal information through our services.

No Automated Decision-Making and Profiling. As part of the Service, we do not engage in automated decision-making and/or profiling, which produces legal or similarly significant effects.

Your rights

General. European data protection laws give you certain rights regarding your personal information. If you are located in Europe, you may ask us to take the following actions in relation to your personal information that we hold:

- **Access.** Provide you with information about our processing of your personal information and give you access to your personal information.
- **Correct.** Update or correct inaccuracies in your personal information.
- **Delete.** Delete your personal information 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 information where you have exercised your right to object to processing (see below).
- **Transfer**. Transfer a machine-readable copy of your personal information to you or a third party of your choice.
- **Restrict**. Restrict the processing of your personal information, for example if you want us to establish its accuracy or the reason for processing it.
- **Object.** Object to our processing of your personal information where we are relying on Legitimate Interests – you also have the right to object where we are processing your personal information for direct marketing purposes.
- **Withdraw Consent**. When we use your personal information based on your consent, you have the right to withdraw that consent at any time.

Exercising These Rights. You may submit these requests by email to help@towns.com. We may request specific information from you to help us confirm your identity and process your request. Whether or not we are required to fulfill any request you make will depend on a number of factors (e.g., why and how we are processing your personal information), if we reject any request you may make (whether in whole or in part) we will let you know our grounds for doing so at the time, subject to any legal restrictions.

Your Right to Lodge a Complaint with your Supervisory Authority. In addition to your rights outlined above, if you are not satisfied with our response to a request you make, or how we process your personal information, you can make a complaint to the data protection regulator in your habitual place of residence.

- For users in Switzerland – the contact information for the Swiss Federal Data Protection and Information Commission (FDPIC) can be found here: https://www.edoeb.admin.ch/en/contact-2
- For users in the European Economic Area – the contact information for the data protection regulator in your place of residence can be found here: https://edpb.europa.eu/about-edpb/board/members_en
- For users in the UK – the contact information for the UK data protection regulator can be found here: https://ico.org.uk/make-a-complaint/

Data Processing outside Europe

We are a Swiss organisation, but we have an affiliate in the U.S. and many of our service providers, advisers, partners or other recipients of data are based internationally. This means that, if you use the Service, your personal information will necessarily be accessed and processed outside of Europe. It may also be provided to recipients in other countries outside Europe. Where we share your personal information with third parties who are based outside Europe, we try to ensure a similar degree of protection is afforded to it by making sure one of the following mechanisms is implemented:

- **Transfers to territories with an adequacy decision.** We may transfer your personal information to countries or territories whose laws have been deemed to provide an adequate level of protection for personal information by the Swiss Federal Council, European Commission, or UK Government (as and where applicable) (from time to time).

- **Transfers to territories without an adequacy decision.**
    - We may transfer your personal information to countries or territories whose laws have **not** been deemed to provide such an adequate level of protection.
    - However, in these cases:
        - we may use specific appropriate safeguards, which are designed to give personal information effectively the same protection it has in Europe – for example, standard-form contracts approved by relevant authorise for this purpose; or
        - in limited circumstances, we may rely on an exception, or 'derogation', which permits us to transfer your personal information to such country despite the absence of an 'adequacy decision' or 'appropriate safeguards' – for example, reliance on your explicit consent to that transfer.

    Data processing outside Switzerland

    Personal information subject to the FADP is transferred to the following countries:

    - U.S. (transfer mechanism: standard contractual clauses (including the Swiss Annex)).

You may contact us if you want further information on the specific mechanism used by us when transferring your personal information out of Europe. See the 'How To Contact Us' section above for our contact details.